Systême soft

Программный комплекс Систэм Платформ

Систэм Платформ

Общее описание

Редакция
13

Содержание

1. Назначение и особенности

Документ содержит краткое описание назначения, функционала и особенностей компонентов, входящих в Систэм Платформ. Документ предназначен для специалистов по разработке, внедрению и эксплуатации проектов автоматизации технологических и производственных процессов.

Систэм Платформ разработана российским производителем программного обеспечения с применением современных подходов, успешно применяемых в IT-сфере.

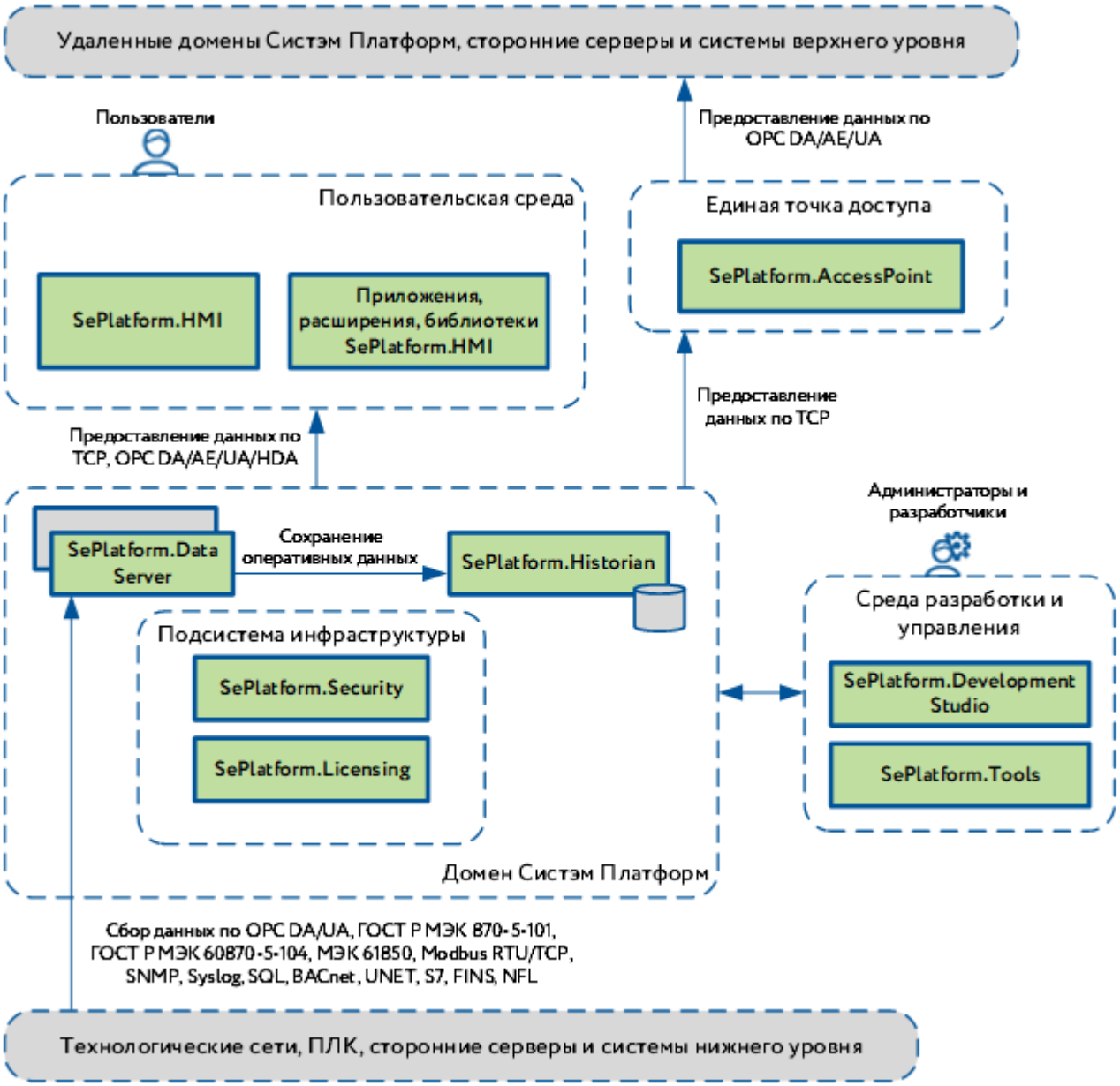
Систэм Платформ включает различные компоненты, используемые для разработки, исполнения и сопровождения проектов автоматизации технологических и производственных процессов. Проекты автоматизации, разработанные с помощью инструментов Систэм Платформ, могут внедряться на локальных и территориально распределенных промышленных предприятиях. Функциональность Систэм Платформ полностью охватывают верхний уровень архитектуры АСУ ТП.

Систэм Платформ является единым программным решением для покрытия всех стадий жизненного цикла проекта автоматизации - начиная от проектирования и заканчивая сопровождением готового проекта.

Возможности Систэм Платформ:

- Современные инструменты разработки, внедрения, эксплуатации и сопровождения проектов автоматизации.
- Возможность работы с единым визуальным инструментом от стадии проектирования до стадии администрирования проекта автоматизации.
- Инструменты контроля согласованности и связанности проекта для исключения ошибок.
- Автоматизированные системы администрирования, развертывания и контроля версионности конфигураций проекта автоматизации.
- Надежные инструменты исполнения проектов автоматизации.
- Инструменты для мониторинга и управления технологическими объектами.
- Инструменты для логической обработки данных.
- Инструменты для сохранения и предоставления полной истории работы системы.
- Инструменты для визуального представления данных пользователю (мнемосхемы, таблицы, графики).
- Возможность интеграции встраиваемых компонентов Систэм Платформ в сторонние программные продукты.

2. Архитектура Систэм Платформ



Ключевой единицей инфраструктуры Систэм Платформ является домен - совокупность вычислительных средств для исполнения проекта автоматизации. Серверные компоненты домена выполняют целевые функции проекта: сбор данных от нижестоящих систем, логическую обработку данных, предоставление данных вышестоящим системам, хранение исторической информации и прочее. К подсистеме исполнения относится SePlatform.Data Server и SePlatform.Historian.

SePlatform.AccessPoint - единая точка доступа, объединяющая серверные компоненты и удалённые домены Систэм Платформ (для построения распределённых систем), а также взаимодействие со сторонними приложениями и системами по стандартным протоколам и спецификациям.

Пользовательская среда обеспечивает работу с визуальной частью проекта автоматизации. К компонентам пользовательской среды относится SePlatform.HMI.

Среда разработки и управления служит для создания, тестирования и отладки приложений и состоит из продуктов SePlatform.Development Studio и SePlatform.Tools. Среда используется также для выполнения централизованных задач по настройке и обслуживанию домена Систэм Платформ.
К подсистеме инфраструктуры относятся продукты SePlatform.Security (регламентирует безопасность и разграничение прав внутри домена), SePlatform.License Server (обеспечивает лицензирование продуктов внутри домена).

3. SePlatform.Data Server

SePlatform.Data Server - компонент Систэм Платформ, выполняющий следующие задачи:

- Сбор данных с устройств в ходе мониторинга контролируемых объектов.
- Предоставление данных клиентам по различным протоколам и спецификациям.
- Повышение надежности проекта за счёт резервирования.
- Логическая обработка данных в режиме реального времени.
- Генерация событий и тревог на основе полученных данных.

Сервер построен по модульному принципу, что позволяет конфигурировать его в зависимости от выполняемых задач и не создавать лишней нагрузки.

Количество экземпляров сервера на одном компьютере не ограничено, что позволяет использовать сервер в качестве конвертера протоколов или для создания демилитаризованных зон.

3.1. Сбор данных

SePlatform.Data Server обеспечивает опрос источников данных по различным протоколам и спецификациям.

Протокол/Спецификация	**Модуль**
ГОСТ Р МЭК 60870-5-104	IEC-104 Master
ГОСТ Р МЭК 60870-5-101	IEC-101 Master
ГОСТ Р МЭК 61850	IEC-61850 Client
Modbus TCP	Modbus TCP Master
Modbus RTU	Modbus RTU Master
OPC DA	OPC DA Client
OPC HDA	OPC HDA Client
OPC UA	OPC UA Client
TCP	HUB
SQL	SQL Connector
SNMP	SNMP Manager
ICMP	SNMP Manager
Файловый интерфейс	HUB
Syslog	Syslog Server
BACNet	BACnet Client

Протокол/Спецификация	Модуль
FINS	FINS Client
NFL	NFL Client
S7	Siemens S7 Client
UNET	UNET Client
EtherNet/IP	EtherNet/IP Scanner

3.2. Предоставление данных клиентам

SePlatform.Data Server предоставляет данные клиентам по различным протоколам и спецификациям.

Протокол/спецификация	Модуль
ГОСТ Р МЭК 60870-5-104	IEC Slave
ГОСТ Р МЭК 60870-5-101	IEC-101 Slave
Modbus TCP	Modbus TCP Slave
Modbus RTU	Modbus RTU Slave
OPC DA	OPC DA Server
OPC HDA	OPC HDA Server
OPC AE	OPC AE Server
OPC UA	OPC UA Server
TCP	TCP Server
Файловый интерфейс	TCP Server

3.3. Ядро

Ядро SePlatform.Data Server является центральным компонентом сервера. Предназначено для реализации инфраструктуры сервера, интерфейсов работы с модулями, сигналами и их свойствами, остальными подсистемами. Ядро может производить значимые логические вычисления, требующие наибольшей скорости вычислений. Такой подход позволяет значительно повысить производительность работы сервера. Все вычисления производятся по описанным при конфигурировании алгоритмам.

Основные функции ядра SePlatform.Data Server:

- Пересчет значений из физических значений в инженерные и в обратном направлении. При пересчете используются линейная и линейная с изломом зависимости.
- Выполнение алгоритмов по событию, таймеру и расписаниям.
- Управление запуском и остановом модулей при старте и в процессе работы сервера.
- Управление состоянием сервера в рамках резервирования.

- Запись и чтение данных из ОБД.
- Управление модулями, отправка и принятие уведомлений об изменении значений сигналов.

3.4. Резервирование

SePlatform.Data Server реализует два вида резервирования:

- горячее резервирование
- полное дублирование

При горячем резервировании система позволяет настроить репликацию данных между резервируемыми серверами для поддержания оперативной базы данных резервного сервера в актуальном состоянии. Тонкая настройка сервера позволяет ограничивать функции сервера в состоянии резерва в широком диапазоне (полное или частичное отключение опроса и обработки данных).

При полном дублировании, серверы работают независимо друг от друга и оба доступны для работы с клиентами. В этом случае клиентское приложение само решает с каким сервером работать. При реализации крупных распределенных проектов с организацией резервируемых пунктов управления возможно создание единой системы резервных пар серверов.

3.5. Логическая обработка данных

Одна из первостепенных задач сервера - промежуточная обработка данных. Для повышения производительности работы сервера, все вычисления, производимые при обработке параметров, вынесены на уровень ядра. За внутрисерверные вычисления отвечает модуль логики. Алгоритмы модуля логики составляются на специальном скриптовом языке SePlatform.Om.

Возможности логической обработки данных:

- Пересчет значений из физических в инженерные и обратно (по линейной и линейной с изломом зависимостям).
- Пересчет значений сигналов по формуле.
- Выполнение алгоритмов по событию, таймеру или расписанию.
- Вызов функций из внешних динамических библиотек.
- Перехват генерируемых событий и тревог.

Специфичные задачи логической обработки:

- Разбор буфера для выделения кода технологического объекта и кода события (модуль Data Buffer).
- Опциональное изменение свойств сигнала Value, Quality или Timestamp (модуль Write VQT).

3.6. Генерация событий и тревог

На основе полученных и обработанных данных сервер может по заранее определенным правилам и алгоритмам генерировать и предоставлять пользователям сообщения о событиях и тревогах. Сервер генерирует события по нескольким алгоритмам срабатывания: дискретный переключатель, перечисление, отклонение, по уровню.

Возможности сервера по генерации событий и тревог:

- Генерация событий в рамках спецификации OPC AE.
- Предоставление информации о событиях в рамках спецификации OPC DA.

- Отправка информации о событиях по электронной почте (Модуль рассылки событий).

3.7. Прочие возможности SePlatform.Data Server

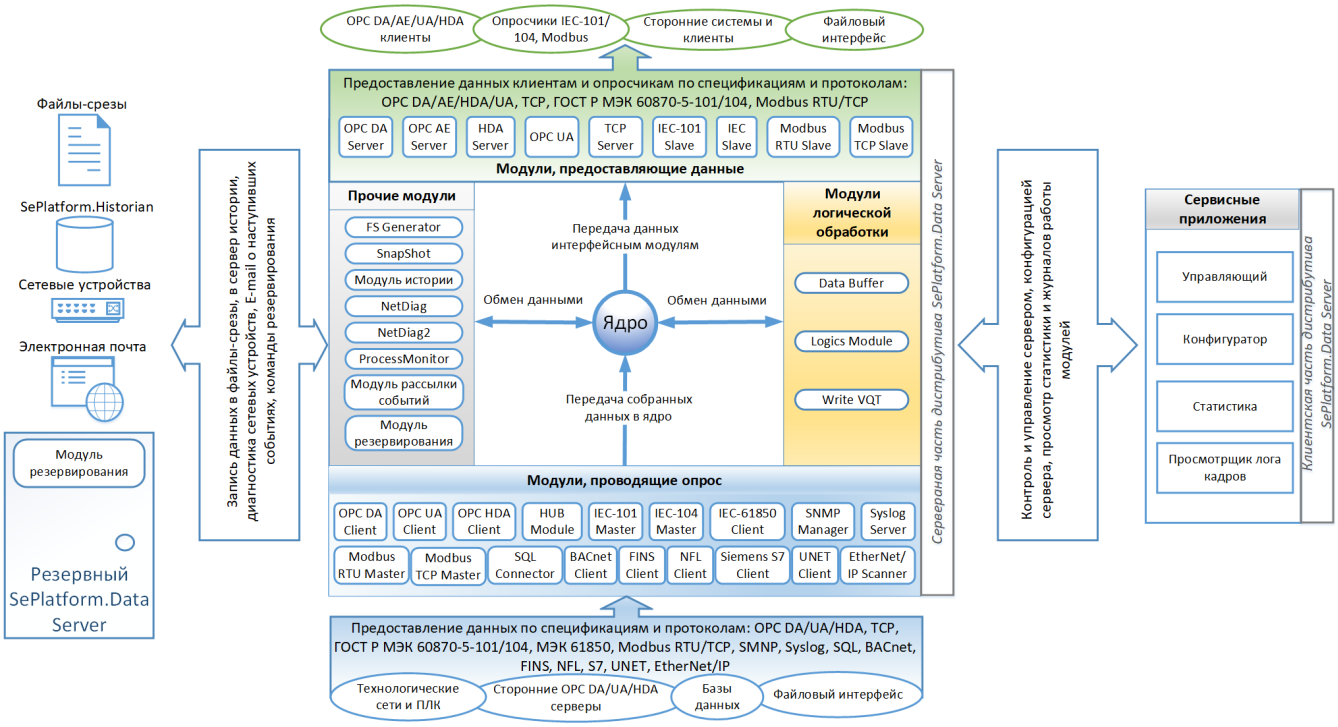
- Сохранение текущих значений сигналов в файл-срезы XML-формата (модуль SnapShot).
- Сохранение текущих значений сигналов в файл-срезы бинарного формата (модуль FS Generator).
- Диагностика сетевых устройств (модули NetDiag, NetDiag2).
- Предоставление данных для записи в сервер истории (Модуль истории).

3.8. Сервисное обслуживание SePlatform.Data Server

Обслуживание сервера выполняется сервисными приложениями, которые входят в состав клиентской части дистрибутива SePlatform.Data Server:

- Редактирование конфигурации сервера выполняется с помощью сервисного приложения Конфигуратор.
- Просмотр статистической информации о работе сервера выполняется с помощью сервисного приложения Статистика.
- Просмотр журналов работы модулей сервера выполняется с помощью сервисного приложения Просмотрщик лога кадров.
- Также для сервисных и диагностических целей при работе с проектами автоматизации применяется набор инструментов SePlatform.Tools.

3.9. Архитектурная схема сервера



4. SePlatform.Historian

SePlatform.Historian - компонент Систэм Платформ для сбора и сохранения информации о технологическом процессе.

Возможности SePlatform.Historian:

- Сбор и хранение оперативных значений параметров технологического процесса.
- Сбор и хранение истории событий и тревог технологического процесса.
- Предоставление исторических данных клиентам.

Модуль истории в составе SePlatform.Data Server выполняет временное хранение данных на стороне сервера и передачу информации в хранилище SePlatform.Historian.

SePlatform.Historian предназначен для управления базами данных и предоставления хранимой исторической информации клиентам по протоколу OPC HDA. Сервер может обслуживать несколько БД одновременно.

Базы данных хранят данные, предоставляемые модулем истории. Используется БД, управляемая SePlatform.Historian. В одну БД могут сохраняться данные с нескольких независимых источников.

4.1. Сбор информации от серверов технологических данных

SePlatform.Data Server обеспечивает сбор, фильтрацию и запись технологических данных в SePlatform.Historian через модуль истории.

Модуль истории в составе SePlatform.Data Server позволяет:

- Указывать технологические параметры, по которым будет вестись история.
- Настраивать фильтрацию записываемых данных по времени и по значению.
- Обеспечить временное хранение данных для записи в файловом буфере при разрывах связи с SePlatform.Historian.
- Записывать данные в несколько резервируемых копий SePlatform.Historian.

Буфер временного хранения данных на стороне SePlatform.Data Server располагается на жестком диске, что предотвращает потерю данных при аварийном отключении компьютера сервера технологических данных. При следующем старте сервера непереданные данные будут повторно отправлены в SePlatform.Historian. Буферизация данных позволяет также сгладить пиковые нагрузки при большой интенсивности получения данных.

4.2. Хранение данных в SePlatform.Historian

Хранение данных ведется в суточных файлах данных для увеличения скорости доступа к данным. Сервер реализует механизмы сохранения и поиска необходимых данных, направленные на обеспечение максимальной производительности работы с дисковой подсистемой компьютера.

Глубина хранения данных ограничена размерами дискового пространства. Скорость записи и чтения данных не зависит от глубины хранения. Запись в сервер – транзакционная. Сервер обеспечивает высокую плотность записи хранимых данных на диск, уменьшая таким образом объемы читаемых с диска данных.

4.3. Резервирование

SePlatform.Historian позволяет формирование резервируемых хранилищ данных. При работе с резервируемыми хранилищами, данные из источника не удаляются, пока не пройдет запись во все хранилища. Поддерживается работа с несколькими резервируемыми хранилищами данных.

4.4. Предоставление данных клиентам

Предоставление данных клиентам осуществляется по:

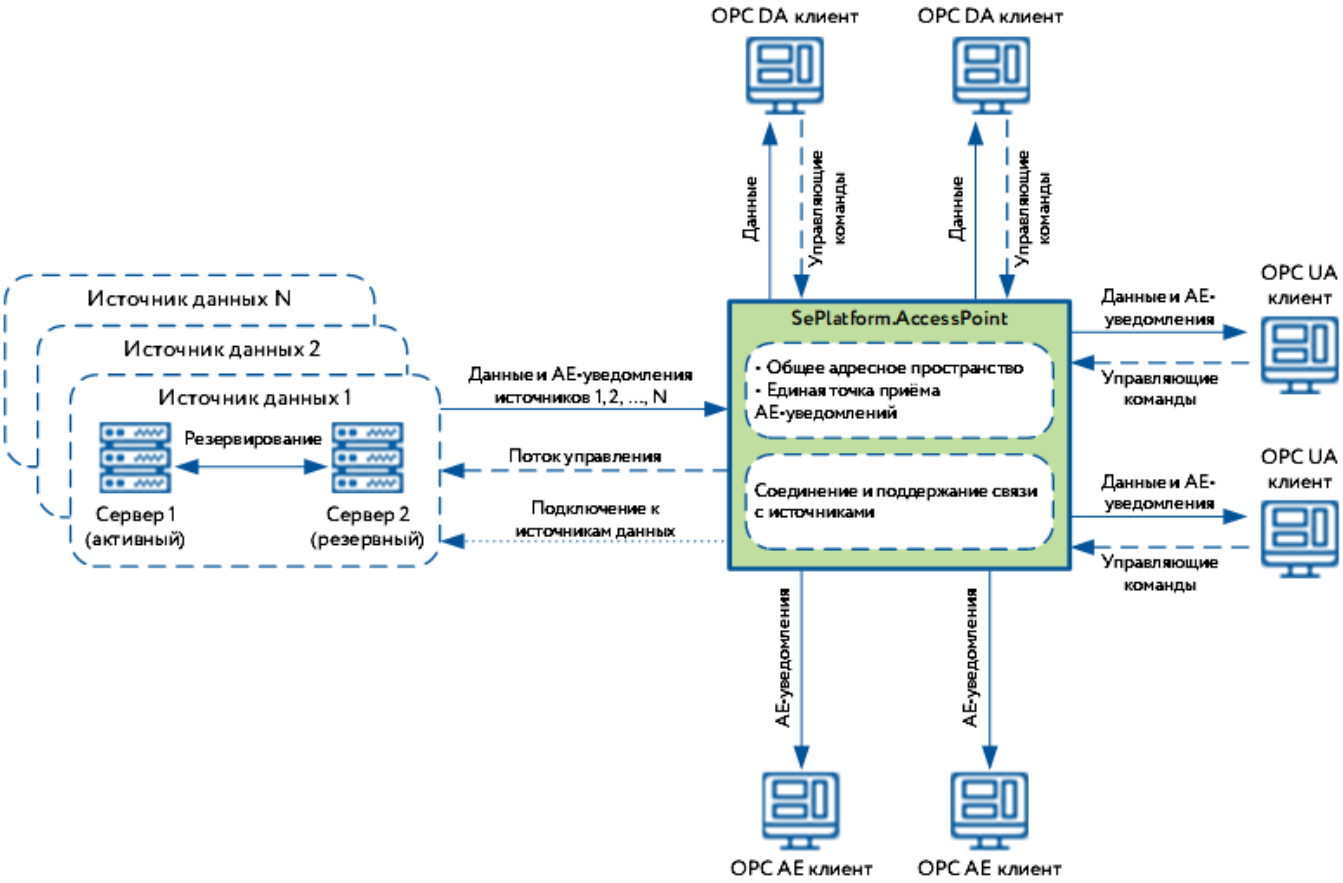
- OPC HDA, SQL и собственному протоколу передачи данных для истории значений технологических параметров.
- SQL и собственному протоколу передачи данных для истории событий.

5. SePlatform.AccessPoint

Компонент реализует функции сервера приложений и межуровневого транспорта. Предназначен для снижения нагрузки на технологические серверы и для транзитной передачи данных между доменами Систэм Платформ.

Возможности SePlatform.AccessPoint:

- Объединение сигналов различных OPC DA-источников в единое дерево сигналов.
- Объединение событий и тревог от различных OPC AE-источников.
- Поддержание связи с источниками данных при разрыве соединения.
- Передача OPC DA и OPC AE данных в виде TCP/IP-трафика в условиях различных сетевых топологий и работа в режиме каскадирования.
- Поддержка сбора данных по файловому интерфейсу.
- Доступ к данным SePlatform.AccessPoint осуществляется по спецификациям OPC DA, OPC AE, OPC UA.



5.1. Объединение адресного пространства серверных компонентов

SePlatform.AccessPoint позволяет объединять адресные пространства серверных компонентов, тем самым обеспечивая связь удаленных доменов Систэм Платформ. Клиенты подключаются к SePlatform.AccessPoint по спецификациям OPC DA, OPC UA и OPC AE как к единой точке доступа.

При построении проектов в нескольких доменах Систэм Платформ в больших распределенных системах есть возможность настраивать подключения отдельных экземпляров SePlatform.AccessPoint друг к другу. Это позволит оптимизировать инфраструктуру системы путем распределения источников данных между экземплярами SePlatform.AccessPoint и снизит нагрузку на каждый SePlatform.AccessPoint.
Возможности SePlatform.AccessPoint по объединению адресного пространства серверных компонентов:

- Объединение адресных пространств нескольких серверных компонентов.
- Постоянное поддержание связи с источниками данных.
- Получение и хранение актуальных конфигураций по каждому серверному компоненту.
- Трансляция измененных значений сигналов в общее адресное пространство.
- Предоставление подписки на общее адресное пространство серверных компонентов для OPC DA клиентов.
- Работа в качестве сервера приложений, который ограничивает нагрузку, создаваемую множеством клиентов при прямых подключениях к источникам данных.
- Обеспечение высокой скорости обмена данными и простой методики конфигурирования в условиях неоднородной сетевой топологии, благодаря использованию протокола на базе TCP/IP.

5.2. Поддержка связи с источником данных

SePlatform.AccessPoint обладает встроенной логикой переключения между серверами и каналами источника данных при разрыве соединения. Данная функция особенно полезна если источник данных представлен резервной парой серверов. SePlatform.AccessPoint автоматически проводит инициализацию всех каналов связи, а затем определяет активный сервер в составе источника данных.

В случае разрыва соединения SePlatform.AccessPoint пытается восстановить связь через резервный канал, если такой имеется. В случае отсутствия резервных каналов в составе активного сервера, SePlatform.AccessPoint переключается на работу с другим сервером и его каналами.

6. SePlatform.Development Studio

SePlatform.Development Studio - среда разработки и администрирования проектов автоматизации.

Возможности SePlatform.Development Studio:

- Сквозное описание физической структуры проекта автоматизации от уровня ПЛК до верхнего уровня.
- Сквозное описание логической структуры проекта автоматизации, а именно функций и данных объектов автоматизации применительно к средствам автоматизации различной функциональной направленности (сервера сбора данных, сервера истории, сервера межуровневого транспорта).
- Представление схемы развертывания проекта автоматизации на исполняющих компонентах.
- Компиляция и сборка конфигураций исполняющих компонентов Систэм Платформ.
- Управление развёртыванием конфигураций проекта в среде исполнения Систэм Платформ.

Среда разработки SePlatform.Development Studio может применяться в проектах автоматизации, построенных на базе Систэм Платформ. При использовании сторонних компонентов в реализации проекта взаимодействие с ними производится по принципу «черного ящика» с определенными входами и выходами.

В основе построения проекта автоматизации с помощью SePlatform.Development Studio лежит объектная модель. Использование принципов такой модели позволяет представить автоматизируемые объекты приложения и компоненты среды исполнения в виде объектов.
Применение объектной модели позволяет:

- Использовать сквозное конфигурирование нескольких проектов.
- Многократно развертывать один проект в различных средах исполнения.
- Повторно использовать части проекта.
- Применять единые средства визуализации.

В SePlatform.Development Studio проект автоматизации разбивается на несколько частей. Выделяются физические объекты и их данные, на основе которых формируется проект приложения. Проект приложения разворачивается в среде исполнения. Описание структуры системы с указанием расположений функциональных узлов, каналов связи и физических серверов называется проектом развертывания. SePlatform.Development Studio позволяет синхронно формировать и модифицировать несколько проектов приложения и развертывания. Благодаря разделению каждого проекта на модули работу над проектом могут вести одновременно несколько пользователей.

6.1. Формирование физической и логической структуры проекта

Объекты физического уровня предназначены для моделирования в проекте структуры физически существующих объектов автоматизации. Структура объектов строится в соответствии с реальной иерархией в материальном мире.
В составе проекта приложения существуют следующие виды объектов:

- Физический объект - определяется в рамках проекта приложения. Может существовать в физическом мире, либо иметь вид вспомогательной структуры без определённого физического выражения.
- Логический объект - представляет собой компонент среды исполнения. Может существовать в физическом мире, либо отражать какой-либо процесс АСУ.

Объекту можно указать его тип. Тип определяет характеристики и поведение всех объектов этого типа. Использование типов позволяет быстро добавлять новые объекты, а также изменять и модифицировать все объекты.
Функции SePlatform.Development Studio в разрезе формирования физической структуры проекта:

- Определение физических и логических объектов проекта автоматизации.
- Определение типов физических объектов и их представлений в средствах автоматизации.
- Выделение логических данных объектов в виде сигналов сервера SePlatform.Data Server.
- Настройка атрибутов входящих и исходящих сигналов.

6.2. Формирование конфигураций средств автоматизации

В схеме развертывания проекта автоматизации каждое средство автоматизации представляет собой сервер ввода/вывода SePlatform.Data Server для возможности демонстрации последовательной передачи данных с устройства на устройство. После построения проекта по каждому средству автоматизации формируются конфигурации серверов SePlatform.Data Server. Конфигурации строятся на основе объектов и их сигналов, привязанных к средствам автоматизации.

На основе представлений физических объектов на логическом уровне появляется возможность просмотреть сформированное адресное пространство вычислительного средства. Адресное пространство доступно для преобразования и приведения к удобному для определения семантики сигналов виду. Иерархия аналогичных узлов адресного пространства строится параллельно. Такая возможность обеспечивается использованием общих групп сигналов, определенных на этапе создания проекта приложения.

Функции SePlatform.Development Studio в разрезе формирования конфигураций средств автоматизации:

- Определение папок дерева сигналов путем добавления представлений физических объектов.
- Формирование набора сигналов и распределение сигналов по папкам дерева сигналов. Добавление сигналов выполняется вследствие привязки объектов к физическим типам, а представлений объектов к представлениям логических типов.
- Формирование перечня свойств сигналов путем назначения атрибутов каждого сигнала внутри сокетов и дополнительных индивидуальных сигналов в представлениях типов.

6.3. Формирование схемы развертывания проекта автоматизации на вычислительных средствах

Проект автоматизации должен содержать схему развертывания проекта автоматизации на вычислительных средствах с указанием протоколов передачи данных. Схема развертывания необходима для определения привязки средств автоматизации к компьютерам, на которых они будут исполняться.

Для имитации средств автоматизации в проекте развертывания формируется перечень вычислительных средств. В составе каждого средства автоматизации определяется набор сетевых адаптеров для обеспечения связи по указанным протоколам. На каждом средстве автоматизации выполняется какая-то отдельная часть соответствующего проекта приложения. В схеме развертывания указывается, какие именно части будут включены в конфигурацию каждого вычислительного средства.

Функции SePlatform.Development Studio в разрезе формирования конфигураций средств автоматизации:

- Создание вычислительных средств для имитации средств автоматизации.
- Привязка модулей проекта приложения к вычислительным средствам для определения набора конфигурации сигналов.

- Настройка адресации сигналов.
- Добавление сетевых адаптеров (модулей SePlatform.Data Server) для каждого средства автоматизации в соответствии с протоколами передачи данных.
- Настройка параметров модулей.
- Настройка связи между вычислительными средствами для обеспечения передачи данных.

6.4. Сборка конфигураций

В результате компиляции проекта выполняется сборка проекта автоматизации и построение выходных конфигураций сервера SePlatform.Data Server.

6.5. Администрирование проекта автоматизации

В рамках администрирования проекта автоматизации, разработанного на базе Систэм Платформ, возможно управлять развертыванием конфигураций в нескольких средах исполнения. Для этого используется единый инструмент управления набором конфигураций всей системы.

Среда разработки SePlatform.Development Studio позволяет распространять построенную конфигурацию на несколько компьютеров одновременно. Процесс установки новых конфигураций называется дистрибуцией. С помощью дистрибуции возможно сократить время настройки и применения конфигураций в рамках большого числа серверов ввода/вывода и рабочих станций, работающих в проекте автоматизации.

Функции SePlatform.Development Studio в разрезе дистрибуции конфигураций:

- Применение разработанной конфигурации в сервер ввода/вывода.
- Подтверждение стабильности текущей конфигурации.
- Возврат к последней стабильной версии конфигурации.
- Индикация различия построенной и текущей конфигураций.

6.6. Командная разработка проекта автоматизации

Проект хранится в виде отдельных папок и файлов. Данная структура хранения даёт возможность одновременной работы над проектом нескольких человек. Рабочая копия каждого файла, расположенная на локальном компьютере, редактируется независимо от других и помещается в единое дерево файлов. В любое время есть возможность открыть ранее сохранённую версию файла. Корректировки и дополнения, внесённые разными разработчиками, могут объединяться и вноситься в одну из версий того или иного файла.

Для одновременной работы с проектом нескольких человек используется TortoiseSVN.

6.7. Характеристики

- При использовании сторонних компонент в реализации проекта взаимодействие с ними производится по принципу «черного ящика».
- Содержимое файлов проекта строится по принципам формата разработки документов `.xml` с учетом объектной модели приложения.
- Работа над проектами ведется как в визуальных редакторах, так и в текстовом виде по выбору пользователя.
- Количество запущенных копий на одном компьютере ограничено производительностью компьютера.

7. SePlatform.Tools

SePlatform.Tools – набор инструментов, предназначенных для сервисных и диагностических целей при работе с проектами автоматизации. В состав дистрибутива SePlatform.Tools входят приложения:

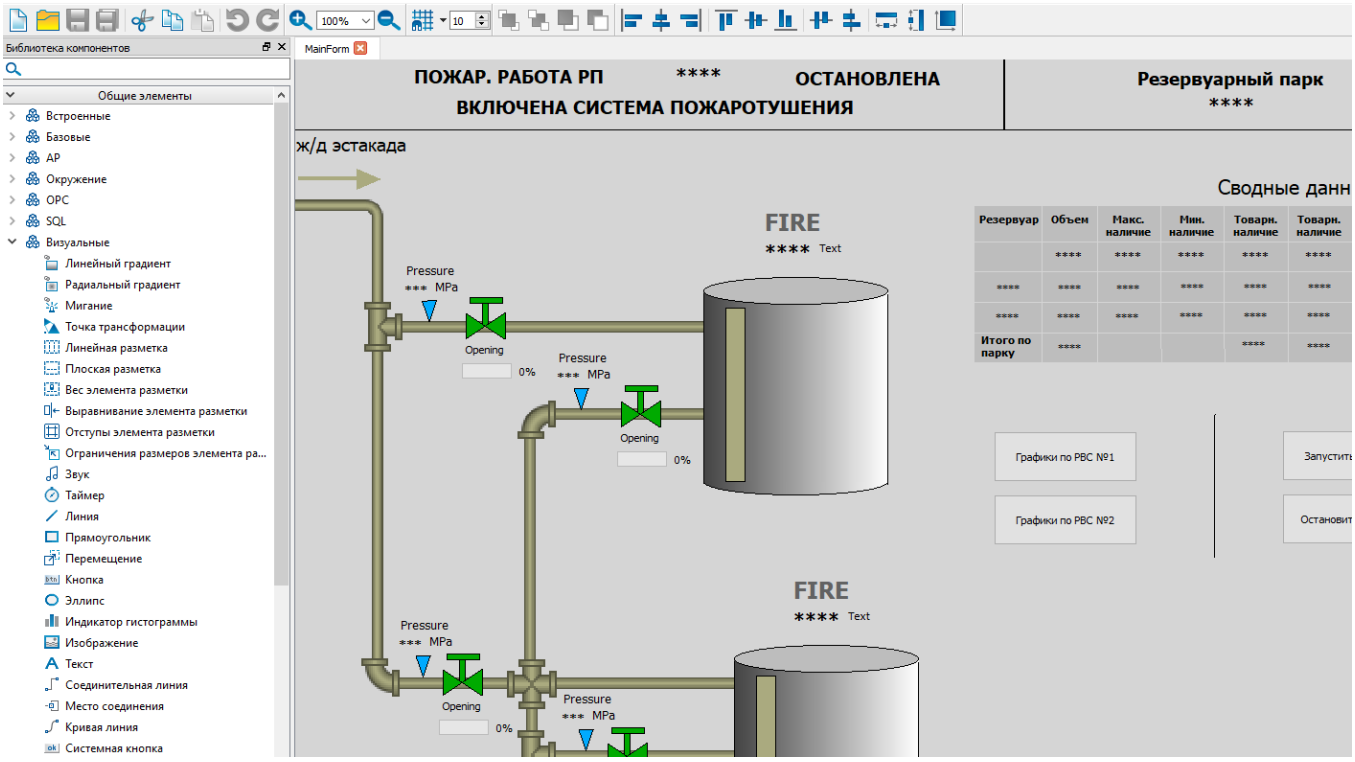
- Приложение Service - LogViewer предназначено для удобного просмотра журналов событий Windows с целью диагностики работоспособности системы.
- Приложение Service - OPCExplorer предназначено для использования в пунктах автоматизации технологических процессов. Применяется для просмотра и изменения значений сигналов, мониторинга событий, возникающих при изменении состояний технологических объектов и для графического отображения изменения значений сигналов.

8. SePlatform.HMI

SePlatform.HMI - среда разработки и исполнения визуальной части проектов автоматизации. Позволяет представлять объекты технологического процесса в виде статических и анимированных объектов мнемосхемы для мониторинга и управления процессом.

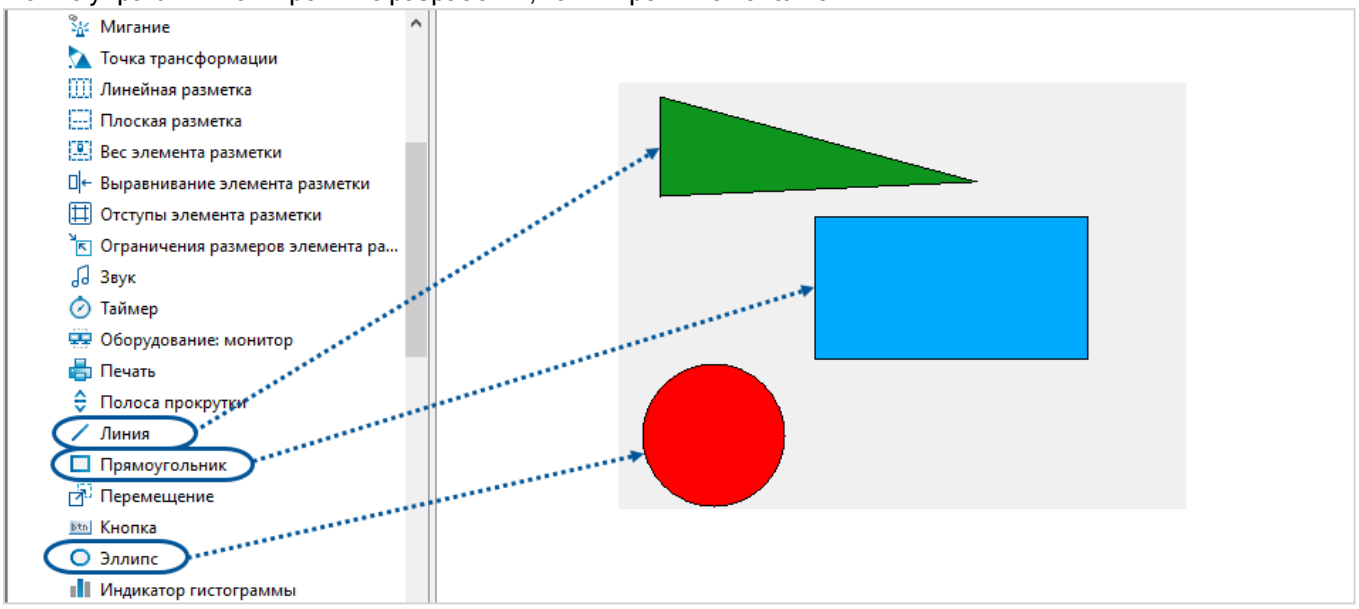
Возможности SePlatform.HMI:

- Визуальный редактор со стандартной библиотекой компонентов для построения мнемосхем;
- Взаимодействие с источником данных среды исполнения;
- Объектно-ориентированный подход при разработке проектов и возможность создания собственных типов графических объектов;
- Поддержка скриптовых языков SePlatform.Om и JavaScript.
- Взаимодействие с подсистемой безопасности SePlatform.Security.
- Взаимодействие с файловой системой, сетевым окружением и оборудованием компьютера.
- Компоненты автоматической разметки элементов мнемосхемы.
- Компоненты организации динамики на мнемосхеме.



8.1. Визуальный редактор для построения мнемосхем

SePlatform.HMI имеет стандартную библиотеку компонентов, позволяющую построить мнемосхему любой сложности. Элементы мнемосхемы могут быть расположены в различных слоях, видимостью которых можно управлять как в режиме разработки, так и в режиме исполнения.



8.2. Взаимодействие с источниками данных

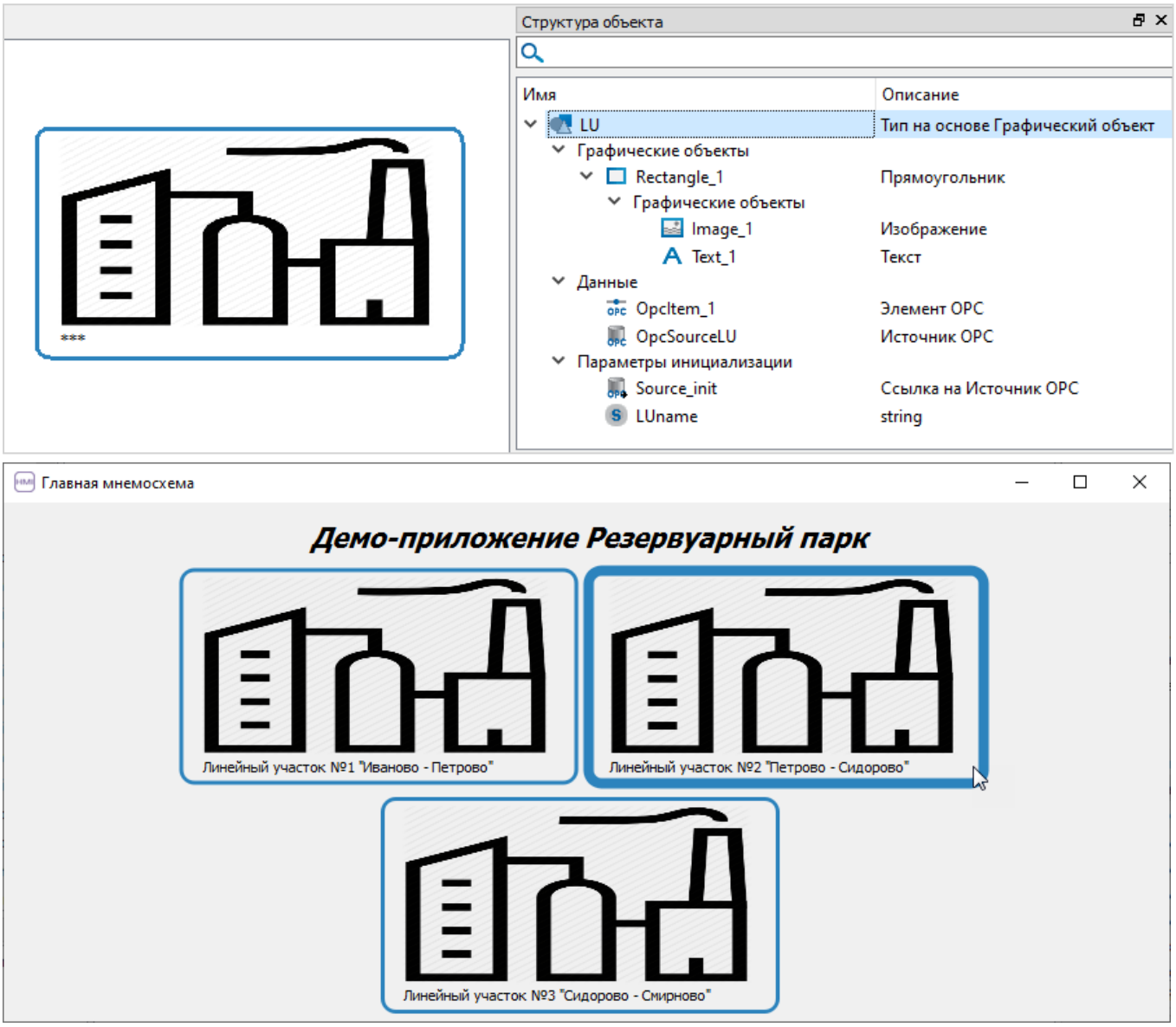
Мнемосхемы, построенные с помощью SePlatform.HMI, позволяют не только визуализировать технологический процесс, но и управлять им.

Получение данных для визуализации и отправка команд осуществляется по стандартным спецификациям, поэтому в качестве источников данных могут выступать не только компоненты Систэм Платформ, но и компоненты других производителей.

SePlatform.HMI поддерживает работу с источниками данных в том числе и посредством скриптового языка, что позволяет реализовать логику любой сложности для управления объектами автоматизации.

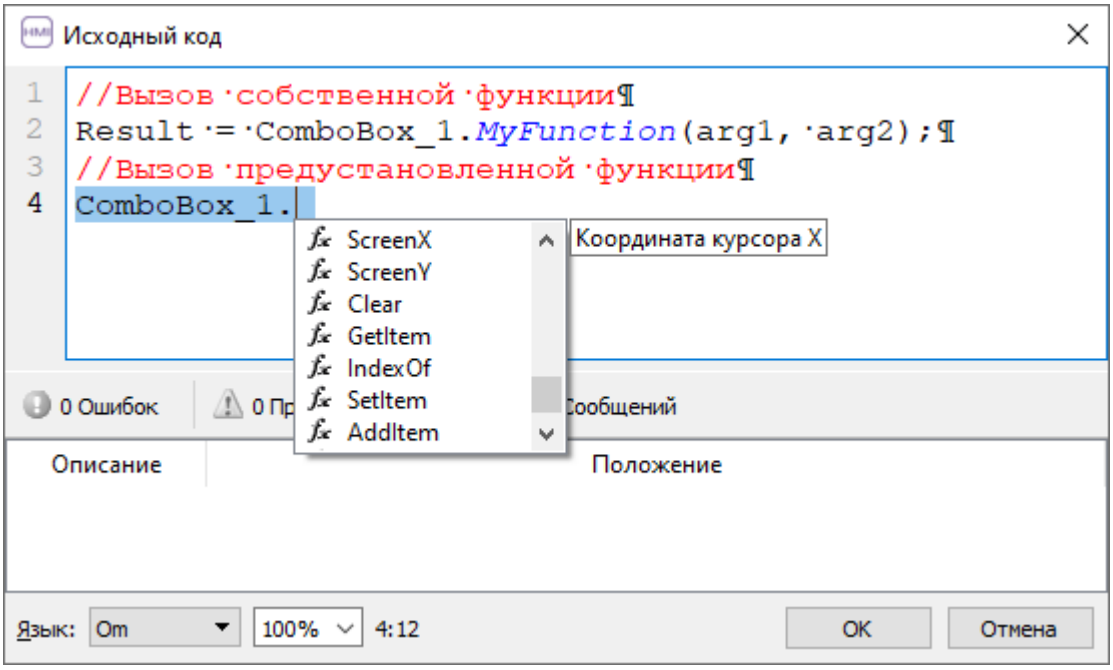
8.3. Объектно-ориентированный подход при разработке проектов

Для многократного применения однотипных объектов на мнемосхемах создаются типы графических объектов. Разработанный единожды тип графического объекта может многократно применяться на разных экранных фомах проекта автоматизации.



8.4. Поддержка скриптовых языков SePlatform.Om и JavaScript

SePlatform.Om является общим скриптовым языком для различных моделей данных продуктов Систэм Платформ. В SePlatform.HMI язык применяется для исполнения формул, обработчиков функций, обработчиков событий и т.д. Скриптовой язык JavaScript применяется для расширения стандартных возможностей языка SePlatform.Om.



8.5. Встраиваемые компоненты

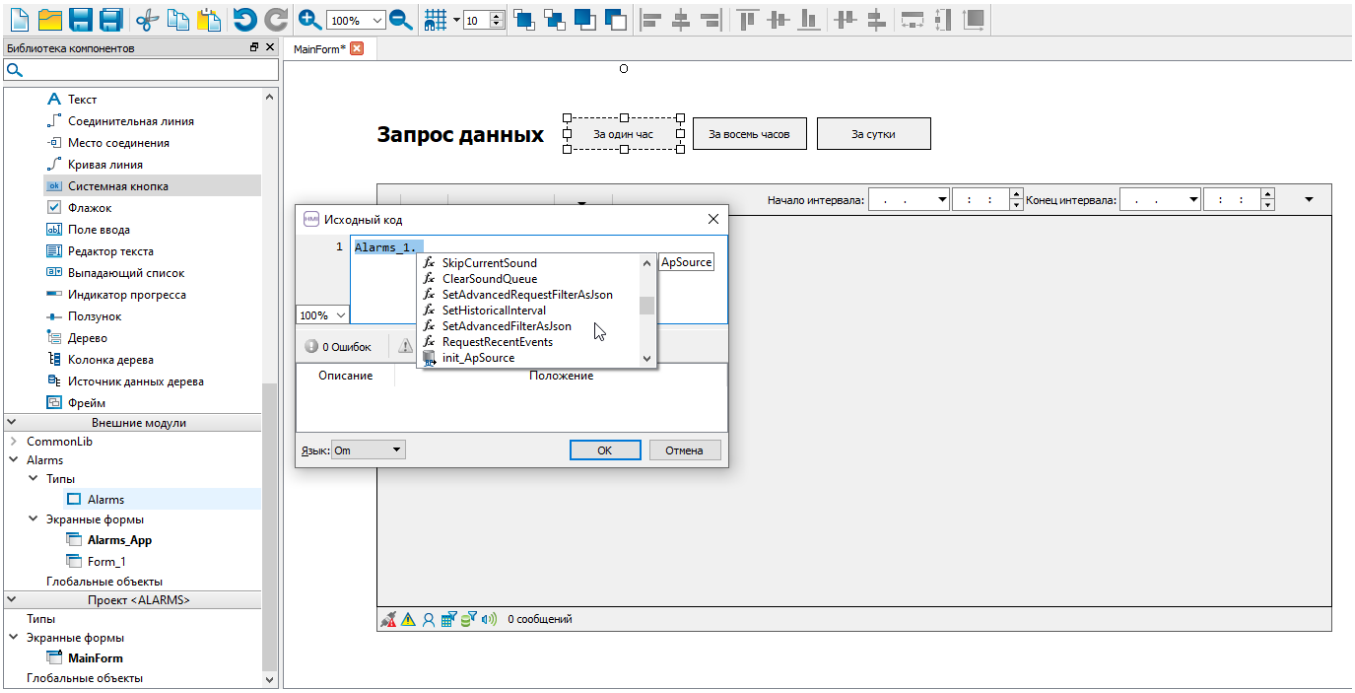
Стандартные возможности внутри проекта SePlatform.HMI можно расширять благодаря встраиванию дополнительных модулей. SePlatform.HMI позволяет подключать к проекту как библиотеки, реализованные средствами SePlatform.HMI, так и внешние .Net библиотеки. Библиотеки, реализованные средствами SePlatform.HMI:

- SePlatform.HMI.CommonLib;
- SePlatform.HMI.Tables;
- SePlatform.HMI.Charts;
- SePlatform.HMI.Security.

Некоторые компоненты, реализованные на базе SePlatform.HMI, возможно использовать как библиотеки, а также запускать как отдельные самостоятельные приложения вне прикладного проекта:

- SePlatform.HMI.Explorer;
- SePlatform.HMI.SecurityConfigurator;
- SePlatform.HMI.IntegrityControl;
- SePlatform.HMI.SetPoints;
- SePlatform.HMI.Alarms;
- SePlatform.HMI.Trends;
- SePlatform.HMI.Statistics.

Это готовые решения с собственным API, дающим возможность гибкой настройки работы компонентов под собственные задачи.



9. SePlatform.HMI.WebViewer

SePlatform.HMI.WebViewer позволяет просматривать мнемосхемы проекта SePlatform.HMI и взаимодействовать с ними через веб-интерфейс.

Функциональные возможности:

- преобразование проекта SePlatform.HMI в веб-приложение с предварительной компиляцией проекта;
- предоставление возможности удаленного доступа к мнемосхемам через веб-интерфейс;
- поддержка возможности подключения к веб-приложению с использованием безопасного соединения;
- предоставление возможности выбора тем оформления веб-приложения.

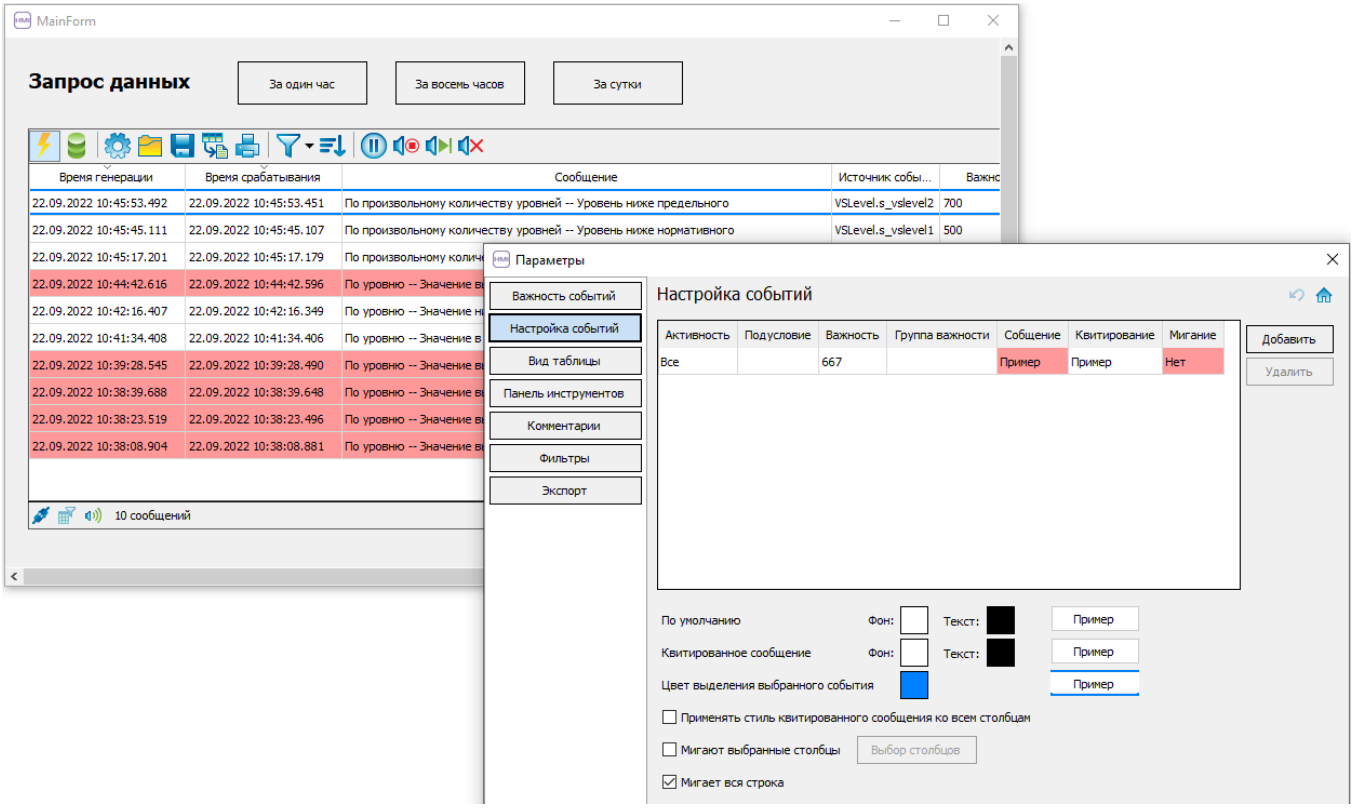
10. SePlatform.HMI - приложения

10.1. SePlatform.HMI.Alarms

SePlatform.HMI.Alarms - расширение среды разработки и исполнения SePlatform.HMI. Представляет собой библиотеку компонентов, позволяющих просматривать сообщения о событиях технологического процесса.

Предоставляемые возможности:

- просмотр оперативных сообщений, получаемых с локальных и удаленных серверов;
- просмотр истории событий;
- настройка звука, цвета и мигания цвета для сообщений о событиях разной важности;
- квитирование оперативных сообщений о событиях;
- фильтрация и сортировка сообщений о событиях;
- экспорт сообщений в файл формата `*.csv`, `*.xlsx` и `*.pdf`;
- печать списка сообщений.



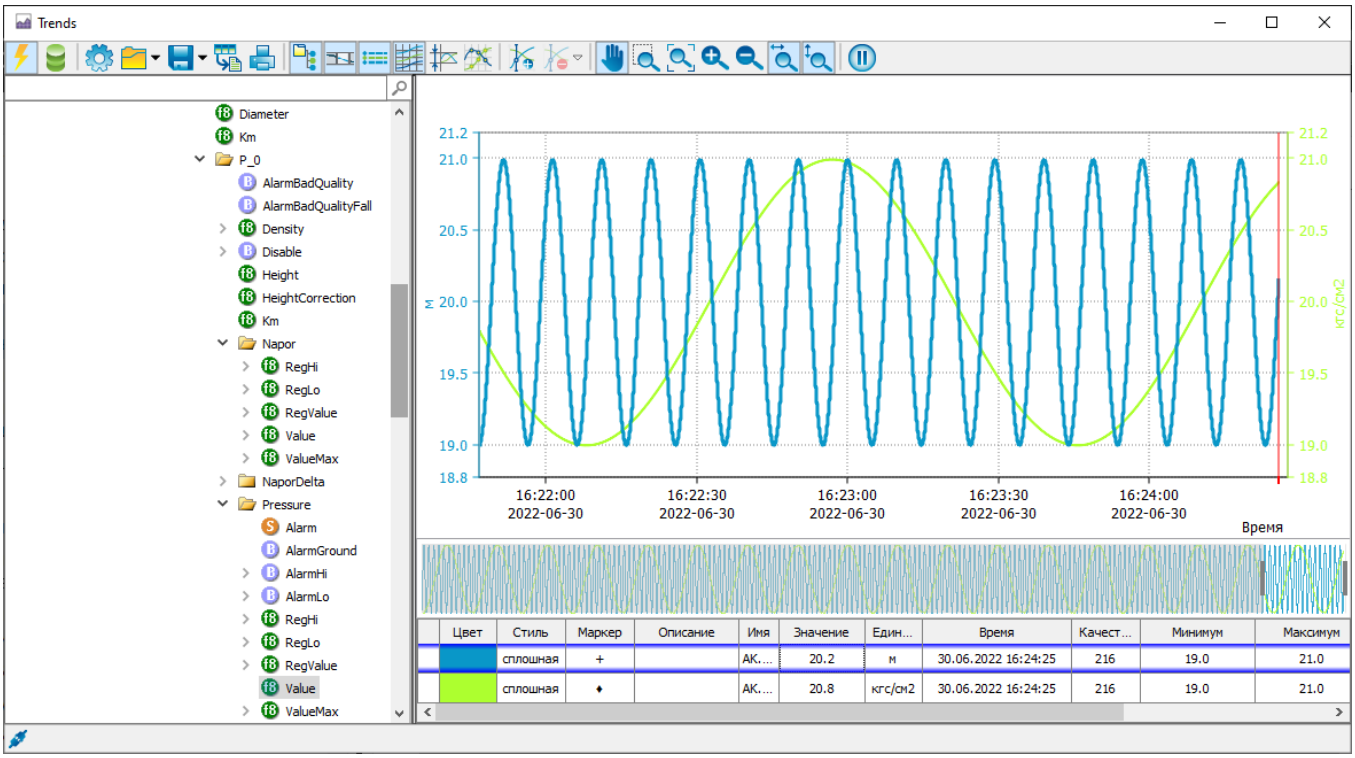
10.2. SePlatform.HMI.Trends

SePlatform.HMI.Trends - расширение среды разработки и исполнения SePlatform.HMI. Представляет собой библиотеку компонентов, позволяющих просматривать графики изменений параметров технологического процесса.

Предоставляемые возможности:

- просмотр графиков изменений параметров в реальном времени;
- просмотр истории значений;

- просмотр данных по сигналам в виде таблицы;
- сохранение списка сигналов и данных по сигналам в файл;
- загрузка списка сигналов и данных по сигналам из файла;
- масштабирование и позиционирование графиков;
- печать графиков.



10.3. SePlatform.HMI.SecurityConfigurator

SePlatform.HMI.SecurityConfigurator - приложение, предназначенное для конфигурирования подсистемы безопасности SePlatform.Security.

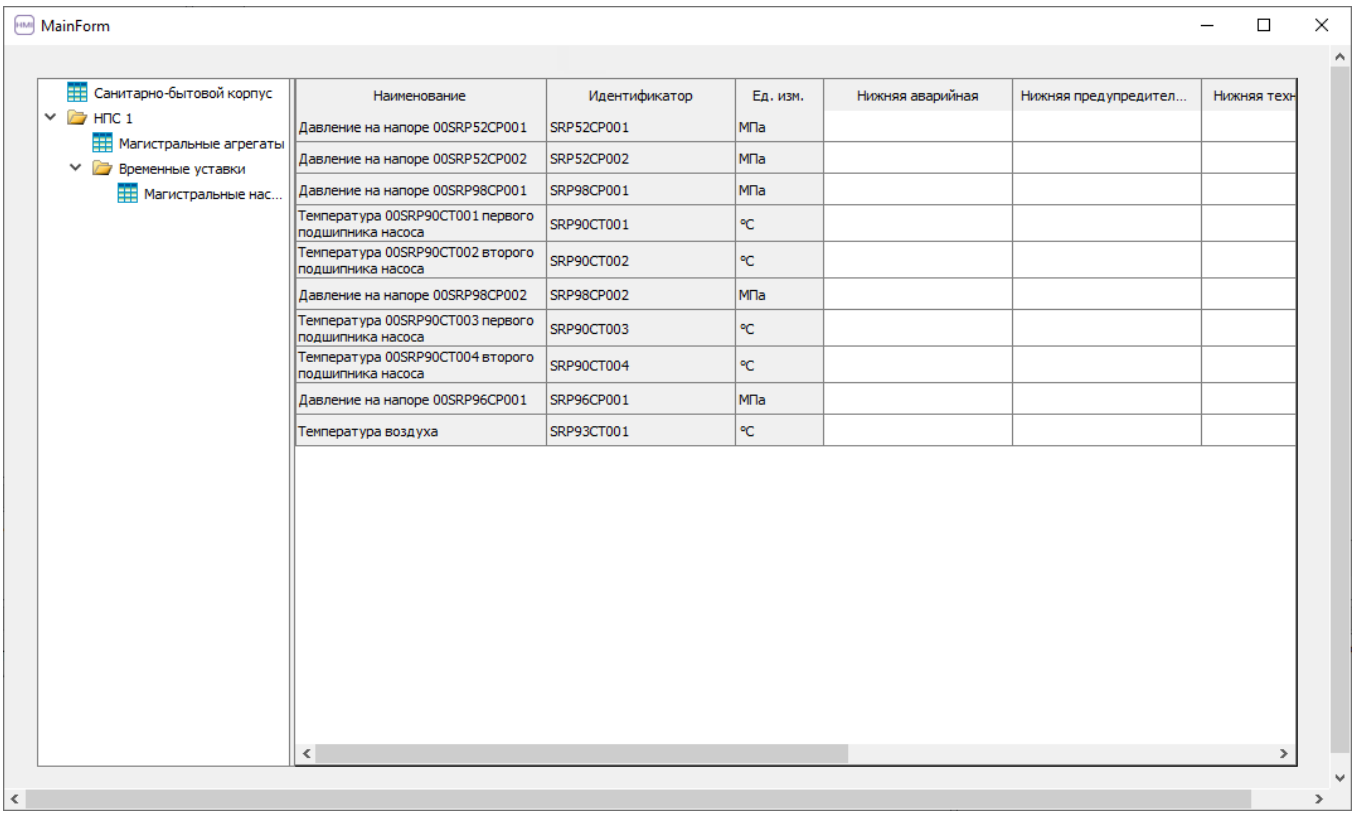
Под конфигурированием подсистемы безопасности подразумевается:

- создание учетных записей пользователей для предоставления им доступа к возможностям проекта;
- объединение пользователей в группы для предоставления им одинаковых возможностей;
- создание прав доступа к возможностям проекта и группировка прав в приложения;
- создание ролей и назначение их пользователям или группам;
- назначение прав пользователям, группам и/или ролям.

10.4. SePlatform.HMI.SetPoints

SePlatform.HMI.SetPoints - приложение для просмотра и редактирования уставок параметров технологического процесса. SePlatform.HMI.SetPoints можно запустить как отдельное приложение, либо встроить его в проект автоматизации, построенный на SePlatform.HMI.

SePlatform.HMI.SetPoints можно встраивать в проекты, работающие на ОС Windows и ОС Linux и доступные через веб-интерфейс.



10.5. SePlatform.HMI.Explorer

SePlatform.HMI.Explorer - прикладное решение на базе SePlatform.HMI, предназначенное для просмотра и изменения значений сигналов SePlatform.Data Server.

10.6. SePlatform.HMI.Charts

SePlatform.HMI.Charts - расширение среды разработки и исполнения SePlatform.HMI. Представляет собой библиотеку компонентов, позволяющих представлять данные, принятые от источника, в виде графиков.

Предоставляемые возможности:

- просмотр графиков оперативных данных по значениям, полученным с локальных и удаленных серверов;
- просмотр графиков исторических данных.

10.7. SePlatform.HMI.Tables

SePlatform.HMI.Tables - расширение среды разработки и исполнения SePlatform.HMI. Представляет собой библиотеку компонентов, позволяющих помещать в таблицу данные об оперативных событиях с источника либо формировать таблицы на основе любых собственных данных.

Предоставляемые возможности:

- заполнение невизуальной таблицы модели данными с источника;
- заполнение невизуальной таблицы модели данными, введёнными вручную, для последующего хранения;

- визуализация таблицы, хранящейся в модели данных;
- декорирование визуальной таблицы.

10.8. SePlatform.HMI.IntegrityControl

SePlatform.HMI.IntegrityControl - приложение для ручного запуска контроля целостности файлов и папок на локальных/удаленных узлах и просмотра результатов проверки. Приложение используется как дополнение к компонентам SePlatform.Security и SePlatform.HMI.Security, т.к. контроль целостности выполняется с помощью этих компонентов.

SePlatform.HMI.IntegrityControl можно запустить как отдельное приложение, либо встраивать его в прикладные проекты, разработанные в SePlatform.HMI. Целевыми проектами могут быть проекты, работающие на ОС Windows, ОС Linux, а также доступные через веб-интерфейс.

10.9. SePlatform.HMI.Statistics

SePlatform.HMI.Statistics – прикладное решение на базе SePlatform.HMI, позволяющее просматривать статистические данные:

- SePlatform.Data Server;
- SePlatform.AccessPoint;
- сервера исторических данных SePlatform.Historian;
- сервера воспроизведения исторических данных SePlatform.Imitator;
- сервера лицензирования SePlatform.License Server.

11. SePlatform.HMI - дополнительные модули

11.1. SePlatform.HMI.Security

SePlatform.HMI.Security – это расширение среды разработки и исполнения SePlatform.HMI. Расширение представляет собой библиотеку компонентов, позволяющих взаимодействовать с подсистемой безопасности SePlatform.Security из проектов SePlatform.HMI.

Под взаимодействием подразумевается:

- регистрация пользователя в подсистеме безопасности (вход) с использованием учетных данных;
- просмотр текущей конфигурации подсистемы безопасности SePlatform.Security;
- изменение текущей конфигурации подсистемы безопасности SePlatform.Security;
- получение информации о статусе операций пользователя;
- выход из подсистемы безопасности;
- контроль целостности файлов.

12. SePlatform.HMI - библиотеки

12.1. SePlatform.HMI.CommonLib

SePlatform.HMI.CommonLib - это расширение среды разработки и исполнения SePlatform.HMI.

Расширение представляет собой библиотеку компонентов, которые можно использовать в своих проектах автоматизации:

- диалоговые окна;
- контекстное меню;
- календарь;
- файловый менеджер;
- конвертер значений;
- дерево сигналов;
- журнал сообщений;
- компоненты безопасности;
- различные кнопки и индикаторы и пр.

Внешний вид и функции компонентов можно настроить с помощью API.

13. SePlatform.Security

SePlatform.Security - подсистема безопасности, позволяющая:

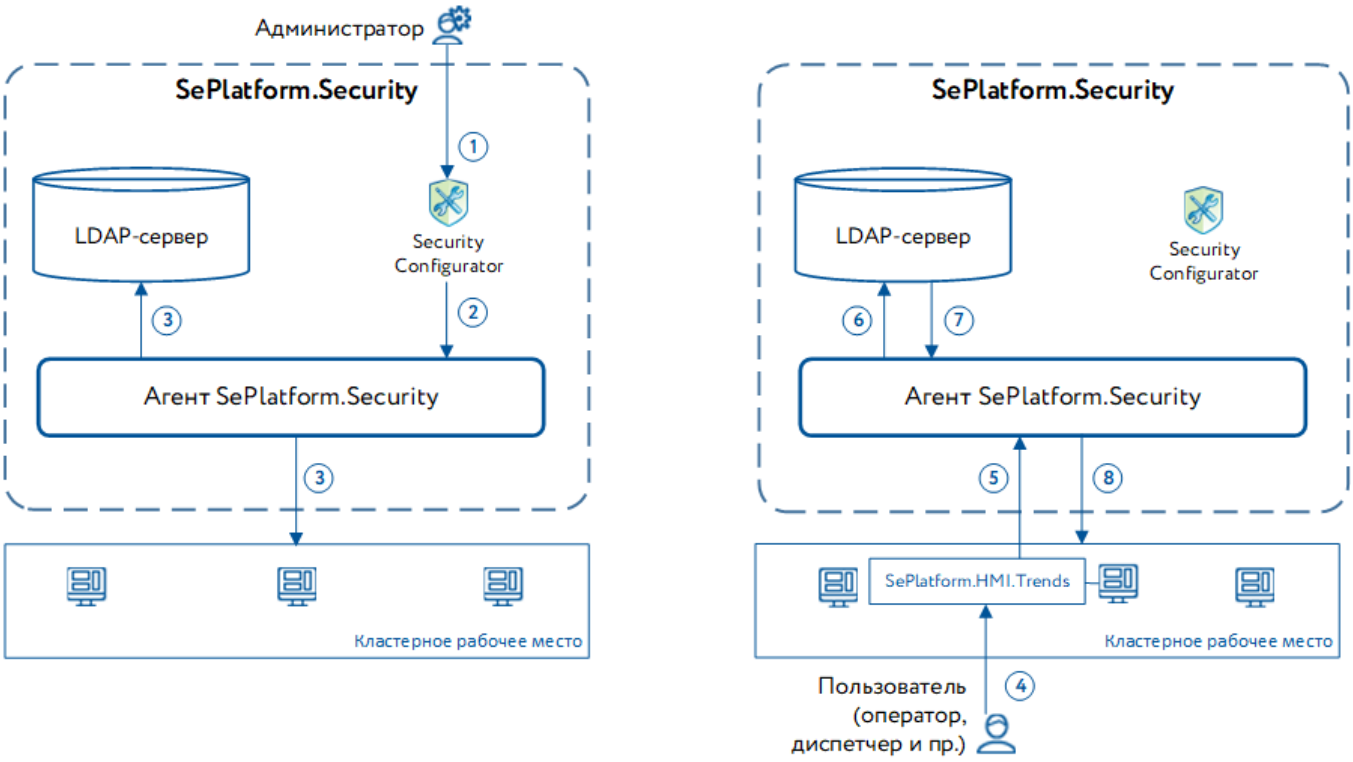
- разграничивать доступ пользователей в проектах автоматизации;
- вести аудит безопасности.

Еще SePlatform.Security позволяет контролировать целостность файлов и папок. Чтобы использовать функцию контроля целостности, понадобится расширение SePlatform.HMI.Security.

SePlatform.Security состоит из следующих компонентов:

- Агент безопасности - служба **`SePlatform.Security.Agent`** (на ОС Windows) или сервис **`seplatform.security.service`** (на ОС Linux);
- LDAP-сервер, предназначенный для хранения информации о пользователях, их правах и пр.;
- Программа для конфигурирования LDAP-сервера - SePlatform.Security.Configurator.

На рисунке показаны примеры взаимодействия компонентов SePlatform.Security. На схеме слева описан процесс конфигурирования подсистемы безопасности администратором (шаги 1-3), на схеме справа - процесс авторизации пользователя в подсистеме (шаги 4-8).



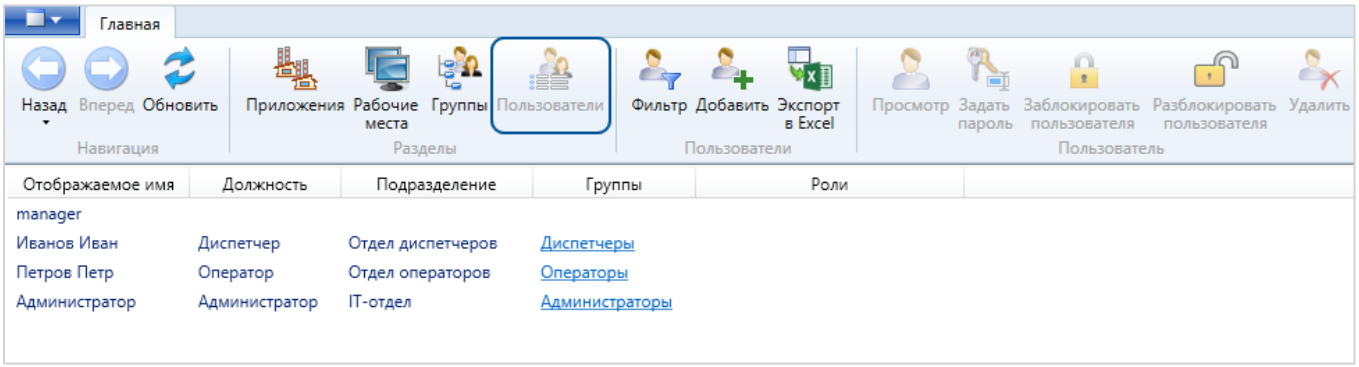
1. Администратор, используя SePlatform.Security.Configurator, создает конфигурацию подсистемы безопасности. Предположим, создает учетную запись пользователя, назначает ему права, и объединяет несколько АРМ в кластерное рабочее место.
2. Эту информацию получает **`SePlatform.Security.Agent`**.
3. **`SePlatform.Security.Agent`** сохраняет полученную информацию на LDAP-сервере в виде записей.

4. Предположим, пользователь, чья учетная запись создана администратором, собирается воспользоваться программой SePlatform.HMI.Trends, установленной на одном из АРМ кластерного рабочего места. SePlatform.HMI.Trends использует сервис безопасности. Поэтому пользователь должен зарегистрироваться в подсистеме безопасности. Для этого он вводит свои учетные данные в окне регистрации SePlatform.HMI.Trends.
5. SePlatform.HMI.Trends передает введенные учетные данные агенту безопасности.
6. **`SePlatform.Security.Agent`** сравнивает введенные данные с записями на LDAP-сервере.
7. Если введенные данные верны, сервер предоставляет агенту информацию о правах пользователя, назначенных ему администратором на шаге 1. **`SePlatform.Security.Agent`** запоминает пользователя как текущего.
8. **`SePlatform.Security.Agent`** предоставляет информацию о пользователе всем программам, использующим сервис безопасности, на всех АРМ кластерного рабочего места, куда у пользователя есть доступ.

13.1. Создание учетных записей пользователей

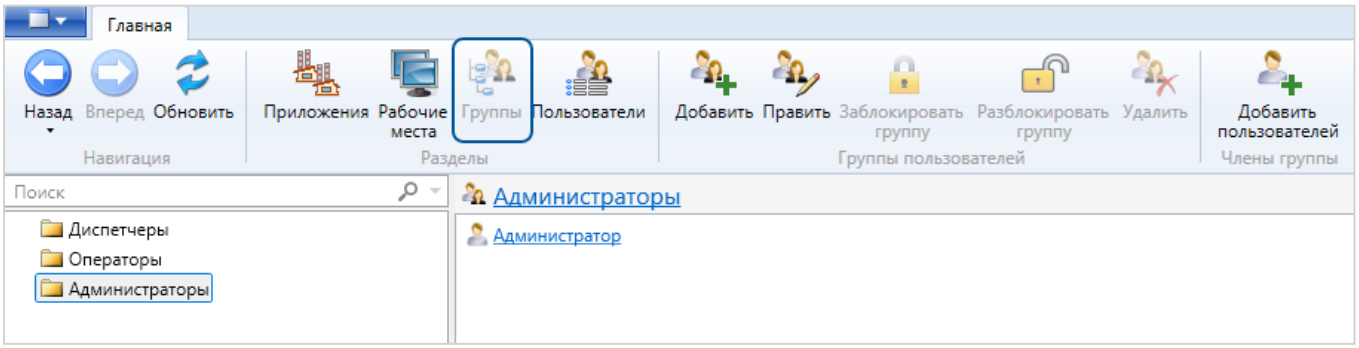
Учетная запись пользователя создается для:

- назначения пользователю прав на определенные действия в проекте автоматизации;
- создания уникальных логина и пароля для доступа пользователя к проекту;
- хранения информации о пользователе - его имени, должности и пр.



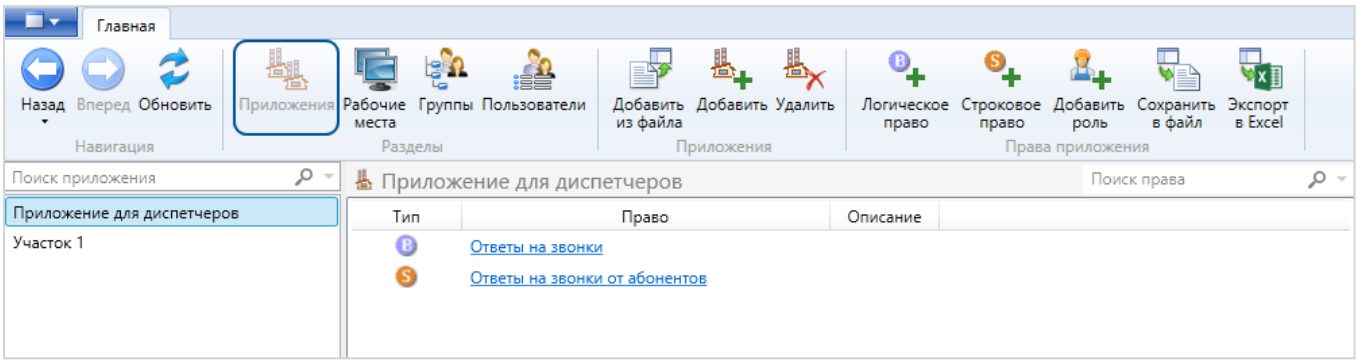
13.2. Работа с группами

Создание групп позволяет объединять пользователей с одинаковыми правами.



13.3. Работа с приложениями

Возможности пользователей в проекте определяются наличием у них разрешений и запретов на определенные действия. Информация о том, разрешено или запрещено пользователю какое-либо действие, хранится виде значения права. Права следует создавать внутри приложений. Приложения позволяют группировать права по какому-либо признаку и создавать роли, которые впоследствии можно назначать пользователям и группам.



14. SePlatform.Domain

Предназначен для выполнения инфраструктурных функций и объединения узлов исполняющих компонентов в единую сеть SePlatform.Net.

Предоставляемые возможности:

- позволяет одновременно разворачивать конфигурацию, построенную с помощью SePlatform.Development Studio, на нескольких экземплярах SePlatform.Data Server и SePlatform.AccessPoint;
- позволяет обновлять конфигурации SePlatform.Data Server и SePlatform.AccessPoint на узлах сети SePlatform.Net;
- мониторинг состояния работы исполняющих компонентов в домене;
- в связке с SePlatform.Security позволяет организовать единую точку доступа в группе распределенных АРМ.

15. SePlatform.Mapping Server

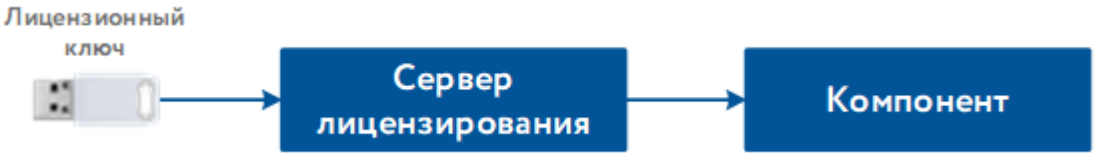
SePlatform.Mapping Server – компонент Систэм Платформ, с помощью которого возможно представление оперативных значений, истории значений и событий в реляционном виде.

Компонент реализован в виде расширения СУБД PostgreSQL и предоставляет SQL-доступ к данным Систэм Платформ, с возможностью изменения оперативных значений.

16. Лицензирование Систэм Платформ

Лицензия даёт пользователю право установки, запуска и использования компонентов Систэм Платформ в проектах автоматизации. Для получения лицензии необходим сервер лицензирования SePlatform.License Server и лицензионный ключ.

Лицензионный ключ содержит набор лицензий на компоненты Систэм Платформ. SePlatform.License Server запрашивает информацию о наличии лицензии на компонент Систэм Платформ в используемом лицензионном ключе. Полученную информацию о лицензии SePlatform.License Server предоставляет компоненту Систэм Платформ.



Существует два типа лицензионных ключей Систэм Платформ: аппаратный и программный.

Аппаратный ключ - это устройство, которое подключается к компьютеру через USB-разъём. Установка драйвера и активация лицензии для аппаратного ключа не требуется. Для лицензирования компонентов Систэм Платформ, установленных на компьютере, достаточно подключить аппаратный ключ в USB разъем данного компьютера.

Программный ключ - это программный аналог аппаратного ключа, который привязывает компоненты Систэм Платформ к конкретному компьютеру. Для лицензирования компонентов Систэм Платформ, установленных на компьютере, требуется активация лицензии.

Для лицензирования компонентов Систэм Платформ используются два вида лицензионных ключей: Sentinel и Guardant.

16.1. Ключи Guardant

Для лицензирования компонентов Систэм Платформ используются два типа ключей: аппаратный ключ Guardant Sign и программный ключ Guardant DL.

16.1.1. ОС Windows

Для лицензирования компонентов Систэм Платформ установите сервер лицензирования SePlatform.License Server.

16.1.1.1. Установка SePlatform.License Server

Для установки SePlatform.License Server запустите установочный файл `SePlatform.LicenseServer.Agent-x.x.x+xx.xxxxx-x64.msi` и следуйте инструкциям мастера установки.

Установка выполняется в папку: `C:\Program Files\SePlatform\SePlatform.LicenseServer.Agent`.

В ОС Windows SePlatform.License Server функционирует в виде службы **`SePlatform.LicenseServer.Agent`**.

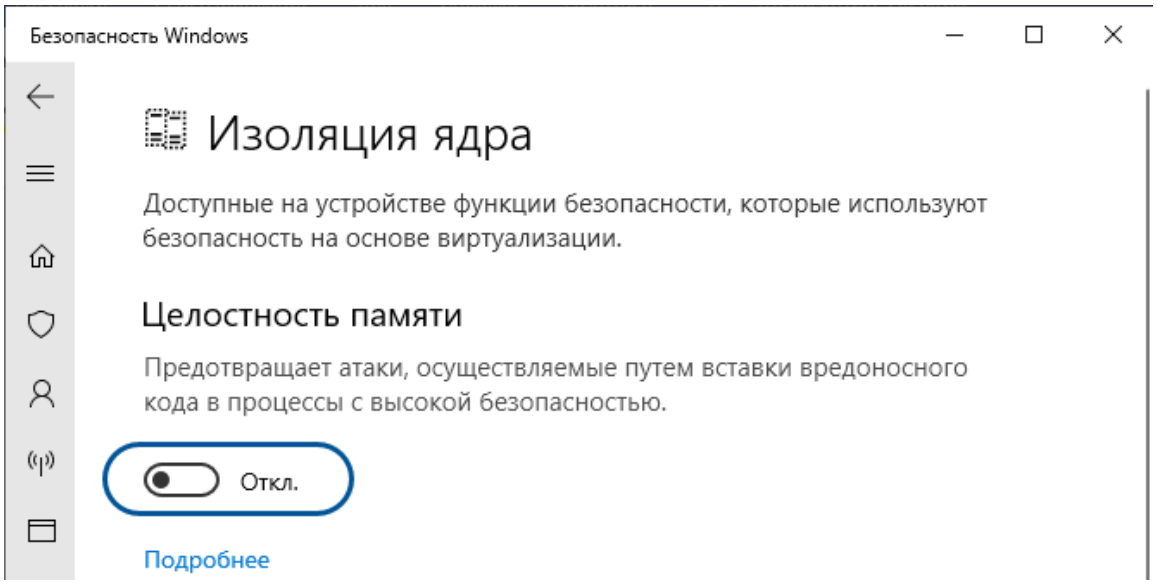
16.1.1.2. Аппаратный ключ Guardant Sign

Подключите аппаратный ключ Guardant Sign в USB разъем компьютера. Дополнительных действий не требуется. Ключ готов к работе.

ОБРАТИТЕ ВНИМАНИЕ

В случае, если компоненты Системы Платформ не могут получить лицензию после подключения аппаратного ключа, то требуется установить драйвер Guardant самостоятельно. Чтобы установить драйвер Guardant:

1. Отключите **«Изоляцию ядра»** в **«Безопасности Windows»**. Для этого:
   1.1. Выполните команду `Пуск → Безопасность Windows`.
   1.2. В открывшемся окне выберите **«Безопасность устройства»**.
   1.3. В разделе **«Изоляция ядра»** нажмите на **«Сведения об изоляции ядра»**.
   1.4. В опции **«Целостность памяти»** передвиньте ползунок переключателя в положение **«Отключено»**.



2. Запустите установочный файл `GrdDrivers.exe` (расположен в папке `\Сторонние компоненты\Guardant\drivers`). Также скачать драйвер для Windows можно со страницы `https://www.guardant.ru/support/users/drivers/`.

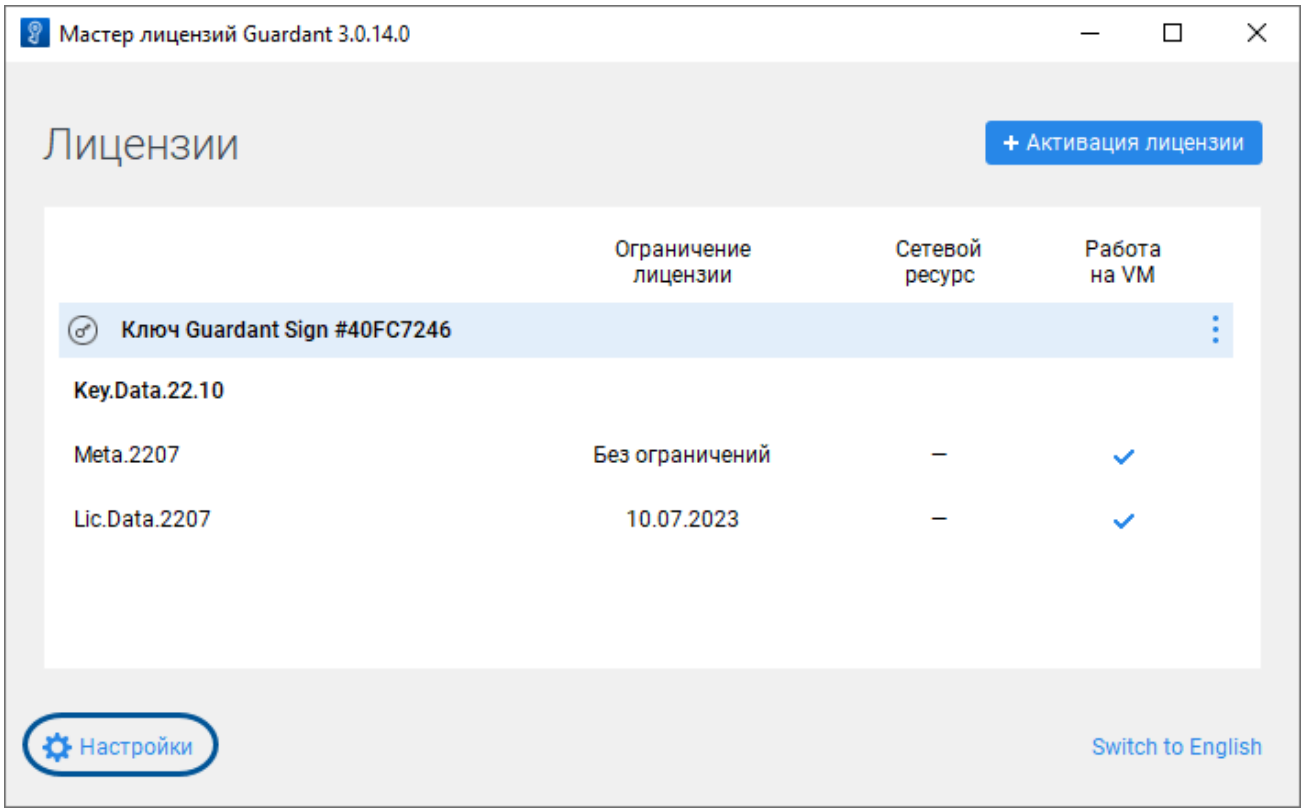
Обновление

ОБРАТИТЕ ВНИМАНИЕ

Для обновления состава лицензии аппаратного ключа Guardant Sign требуется подключение к сети Интернет.

1. Запустите Мастер лицензий Guardant - приложение `license_wizard.exe` (расположено в папке `\Сторонние компоненты\Guardant\x.xx\license_activation`).

2. Перейдите в **Настройки**:

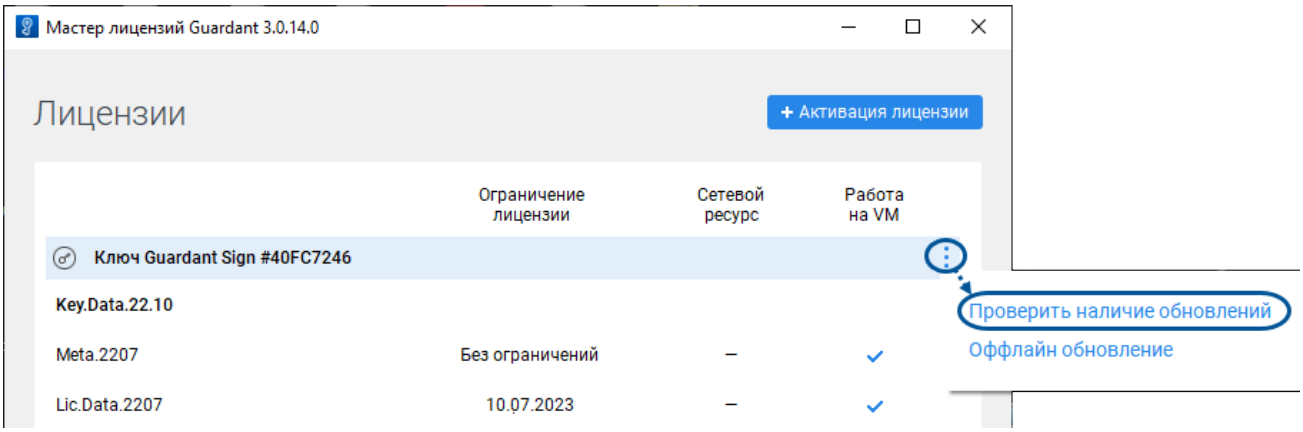


3. Укажите адрес сервера обновления лицензий.

```
https://licsep.systeme.ru:443
```

4. Вернитесь в окно **Лицензии**, нажав **Назад**.

5. В меню ключа выберите команду **Проверить наличие обновлений**.



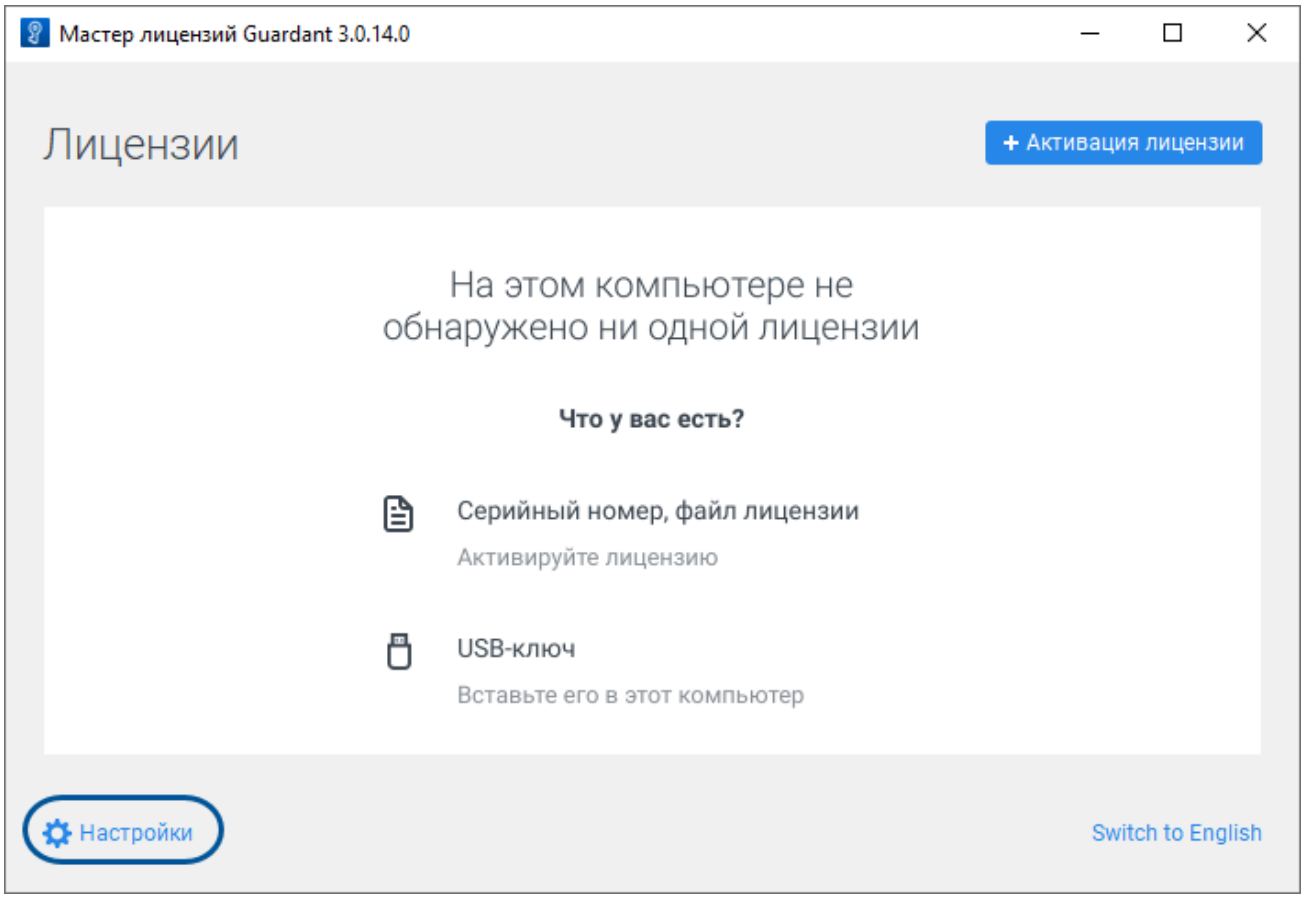
6. Если для ключа будут обнаружены обновления, то они отобразятся в списке **Обновления лицензий**. Для обновления лицензии ключа нажмите кнопку **Применить**.

16.1.1.3. Программный ключ Guardant DL

Активация, обновление и перенос лицензии программного ключа Guardant DL выполняется в приложении Мастер лицензий Guardant - `license_wizard.exe` (расположено в папке `\Сторонние компоненты\Guardant\x.xx\license_activation`).

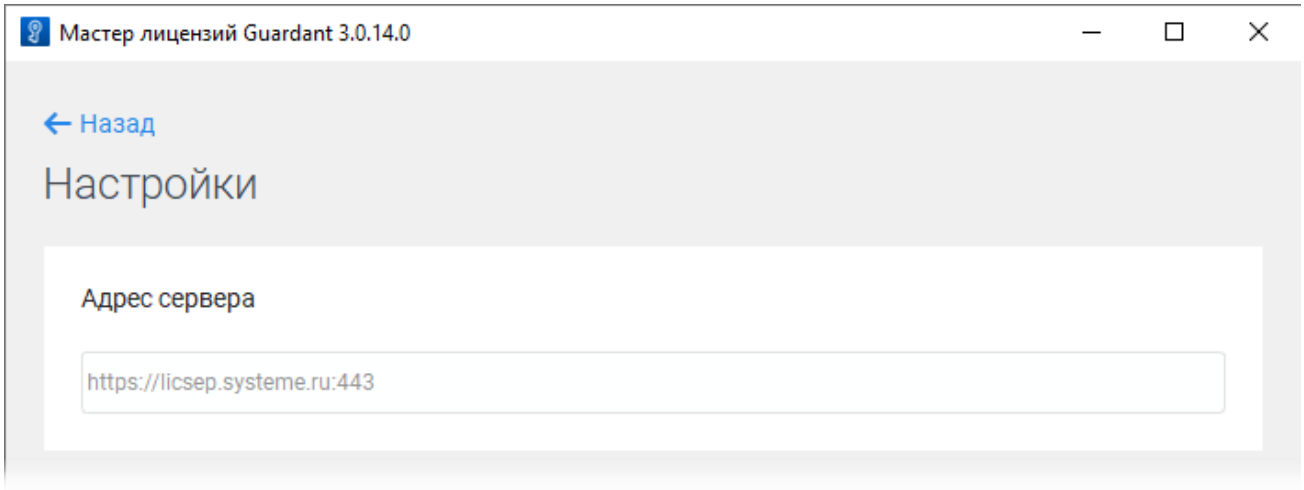
Активация на компьютере с доступом в Интернет

1. Запустите приложение Мастер лицензий Guardant.
2. Перейдите в **Настройки**:



3. Укажите адрес сервера обновления лицензий.

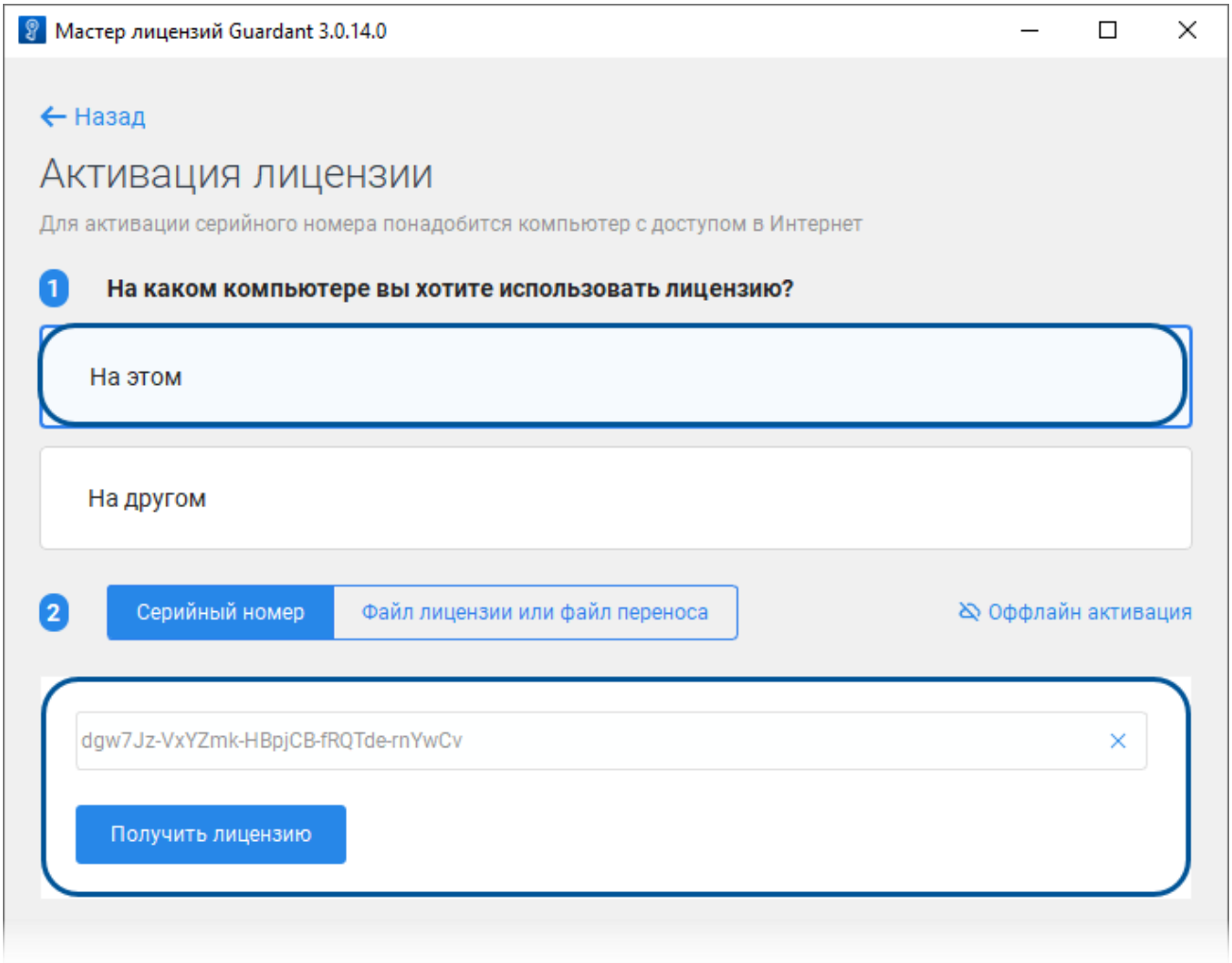
```
https://licsep.systeme.ru:443
```



4. Вернитесь в окно **Лицензии**, нажав **Назад**.

5. В окне **Лицензии** нажмите кнопку **Активация лицензии**.

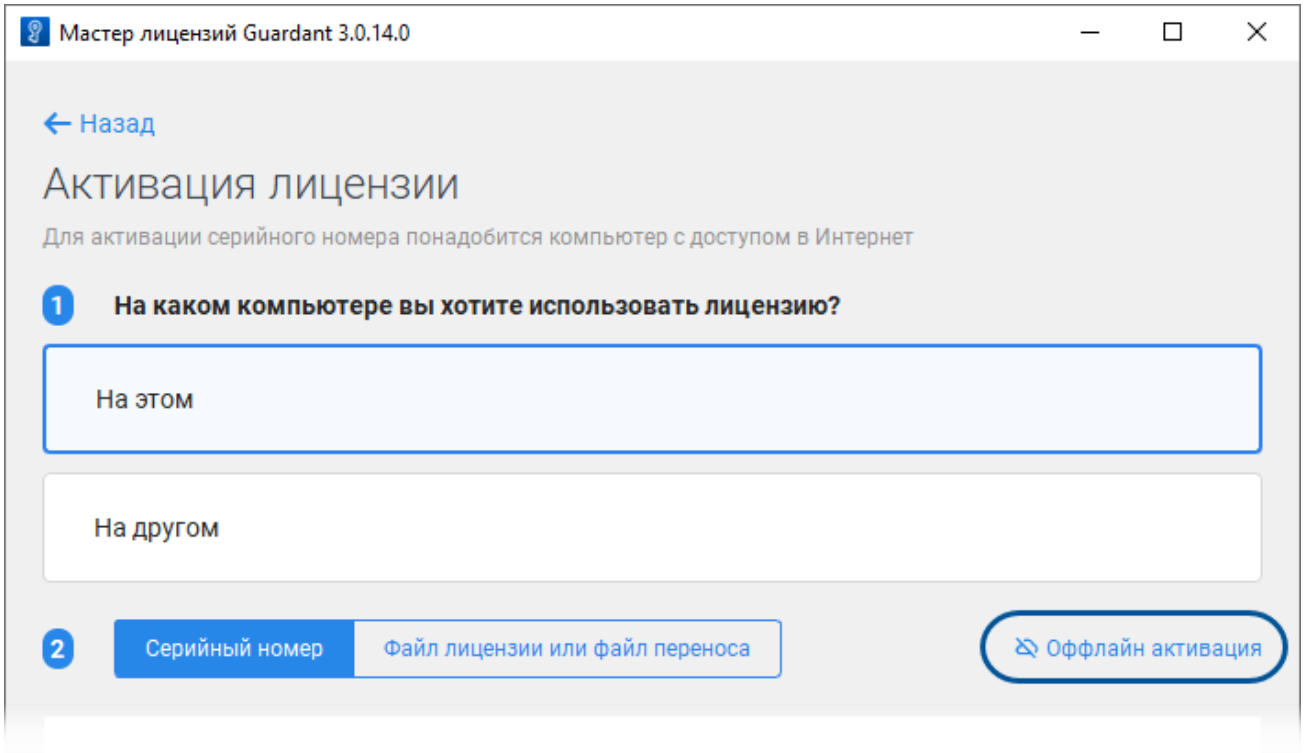
6. В окне **Активация лицензии** выберите компьютер, на котором будет использоваться лицензия - **На этом**, введите в поле ввода серийный номер программного ключа, указанный в сертификате, и нажмите кнопку **Получить лицензию**.



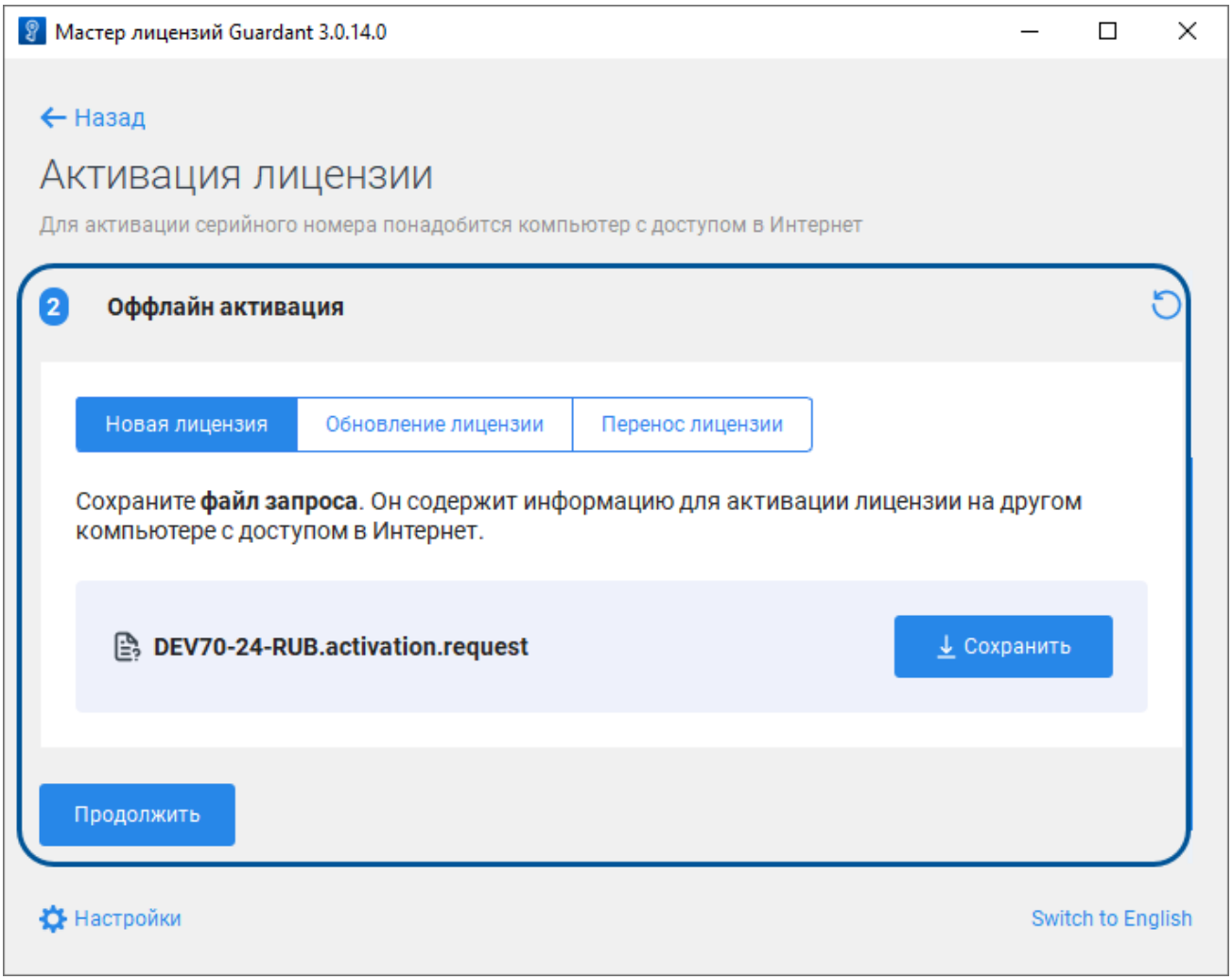
Активация на компьютере без доступа в Интернет

1. Запустите приложение Мастер лицензий Guardant.
2. Нажмите **Активация лицензии**.

3. В окне **Активация лицензии** выберите компьютер, на котором будет использоваться лицензия - **На этом** и нажмите **Оффлайн активация**.



4. На вкладке **Новая лицензия** нажмите кнопку **Сохранить**, сохраните на диске файл запроса формата `*.request` и нажмите кнопку **Продолжить**.

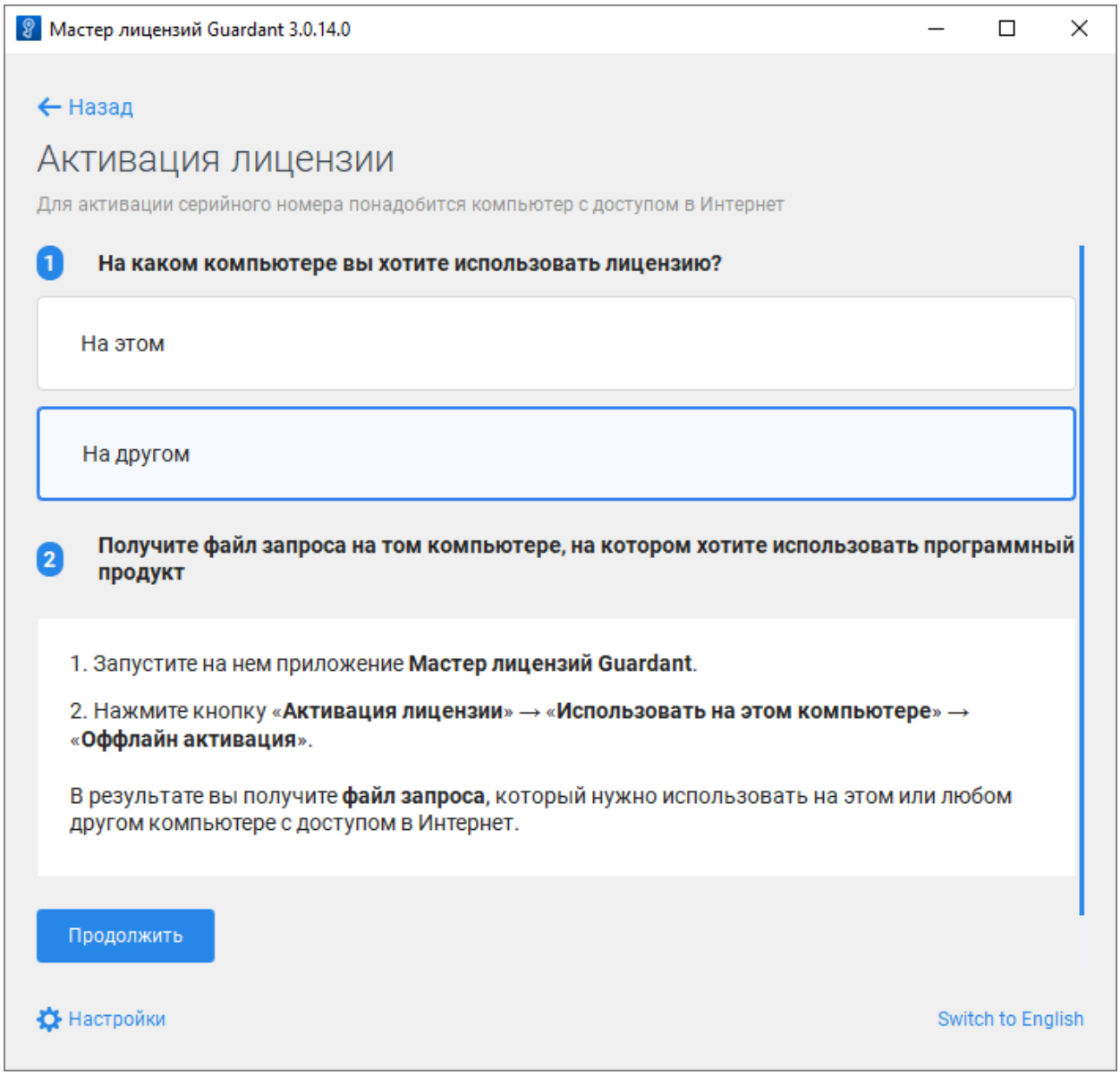


5. Перейдите на компьютер с доступом в Интернет и запустите приложение Мастер лицензий Guardant.
   5.1. Перейдите в **Настройки** и укажите адрес сервера обновления лицензий.

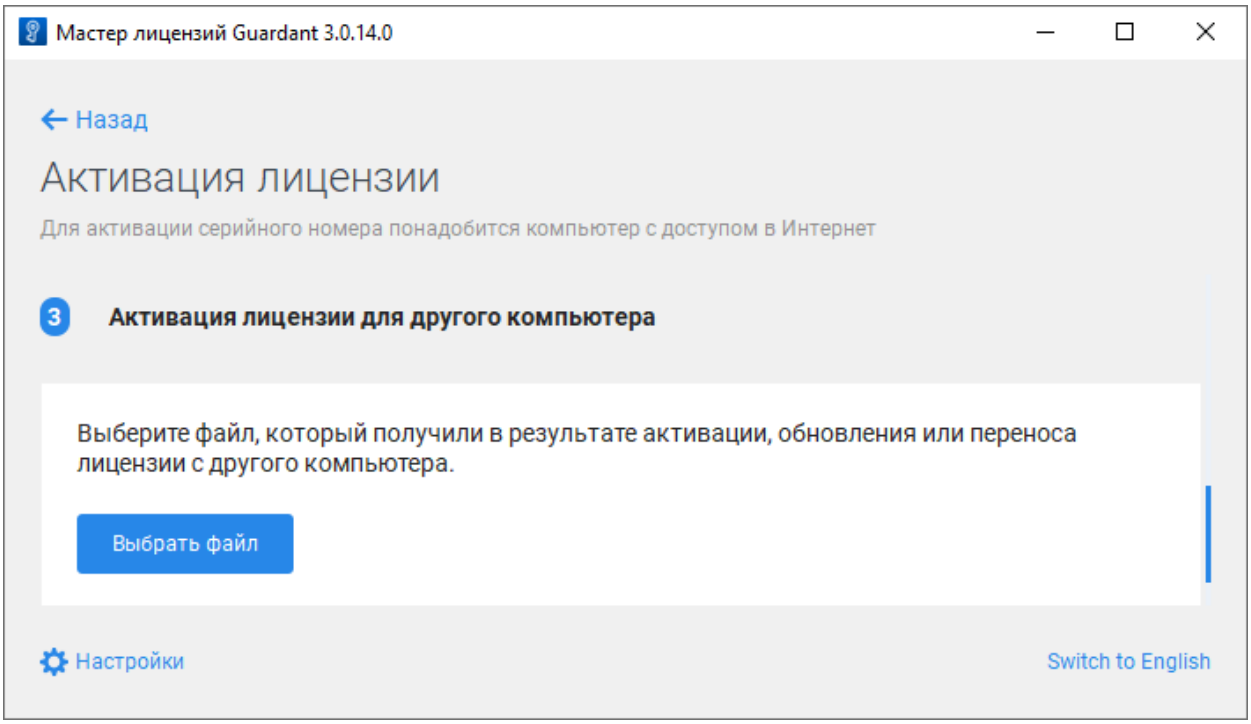
```
https://licsep.systeme.ru:443
```

   5.2. Вернитесь в окно **Лицензии** и нажмите кнопку **Активация лицензии**.

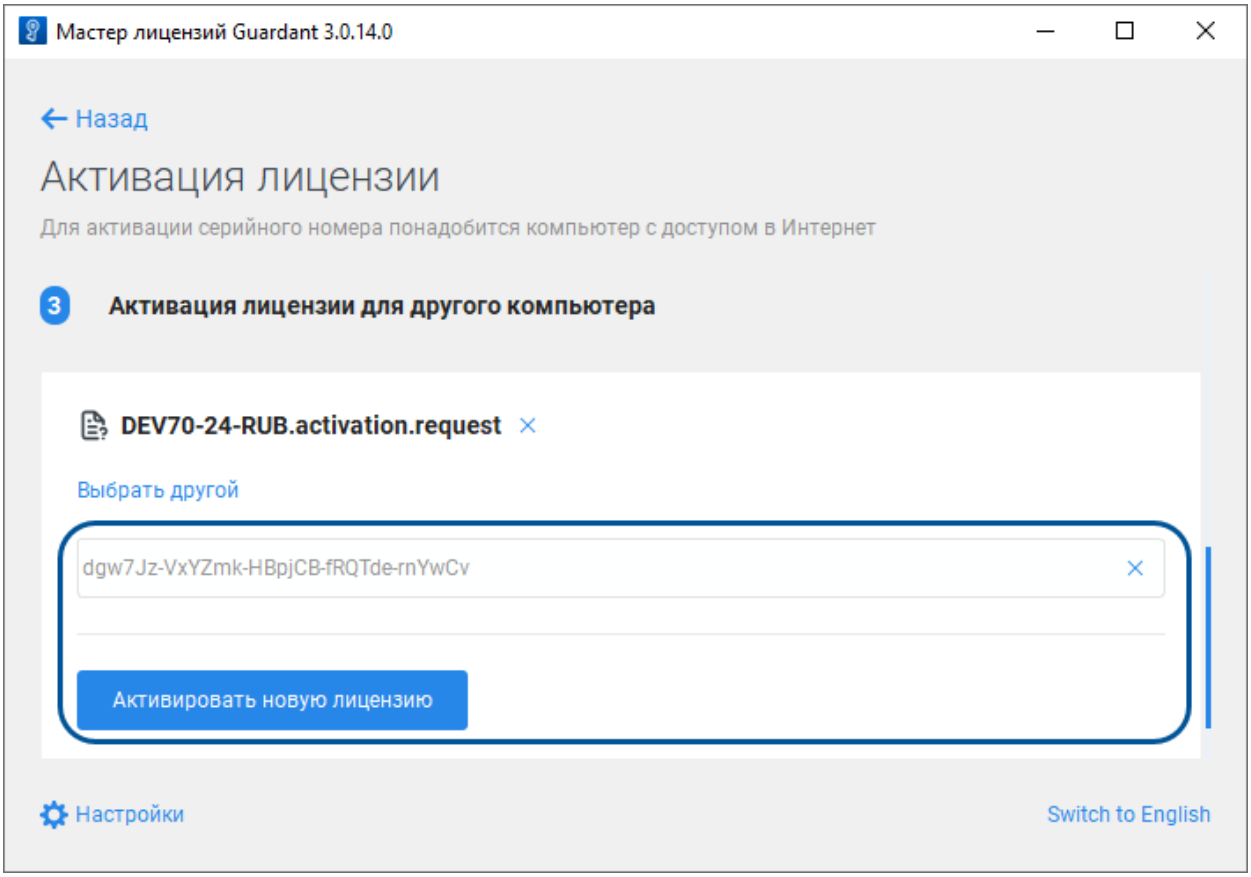
5.3. Укажите компьютер, на котором будет использоваться лицензия - **На другом** и нажмите кнопку **Продолжить**.



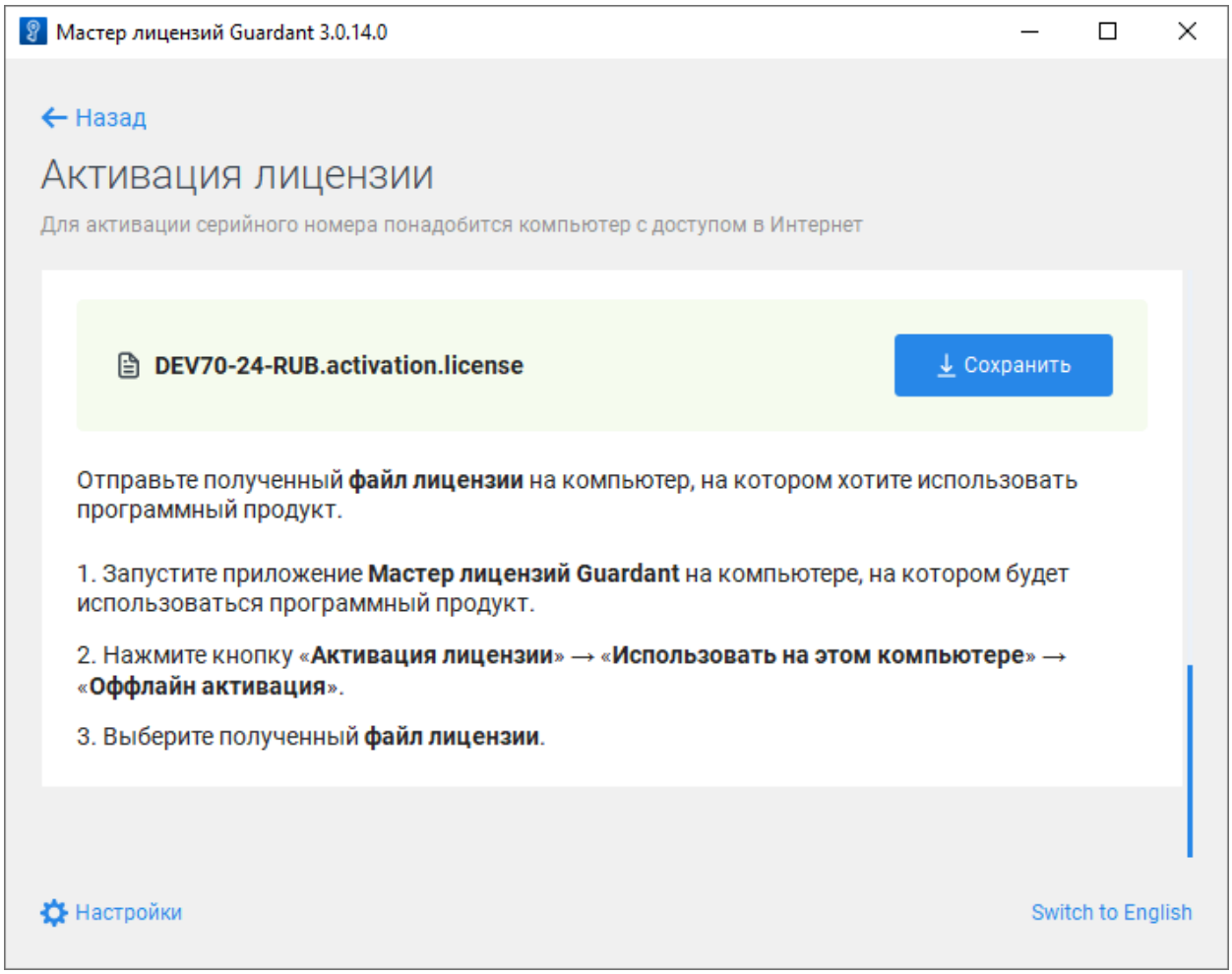
5.4. Нажмите кнопку **Выбрать файл** и выберите файл формата `*.request`, перенесенный с компьютера без доступа в Интернет.



5.5. Введите в поле ввода серийный номер программного ключа, указанный в сертификате, и нажмите кнопку **Активировать новую лицензию**.

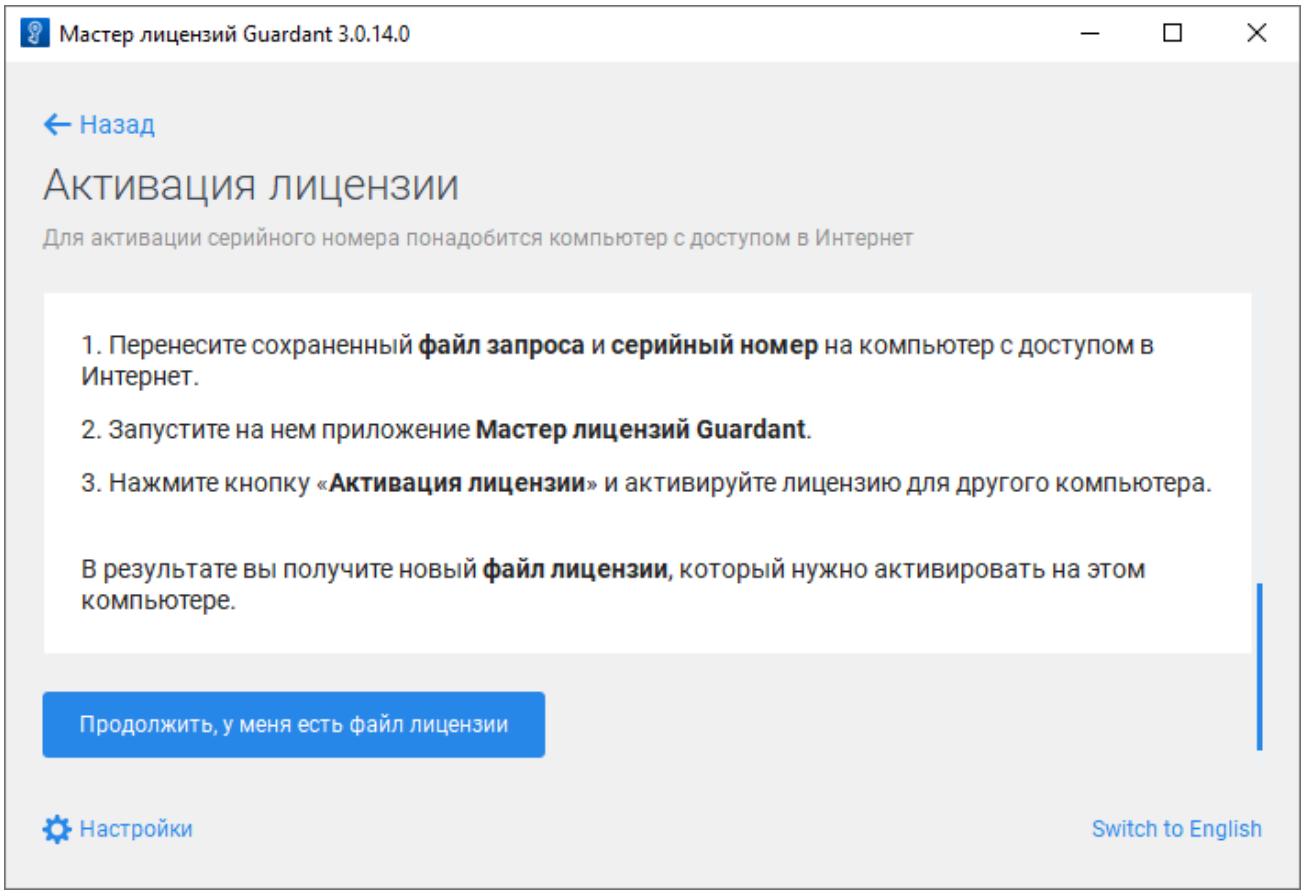


5.6. Нажмите кнопку **Сохранить** и сохраните на диске файл активации лицензии формата `*.license`.

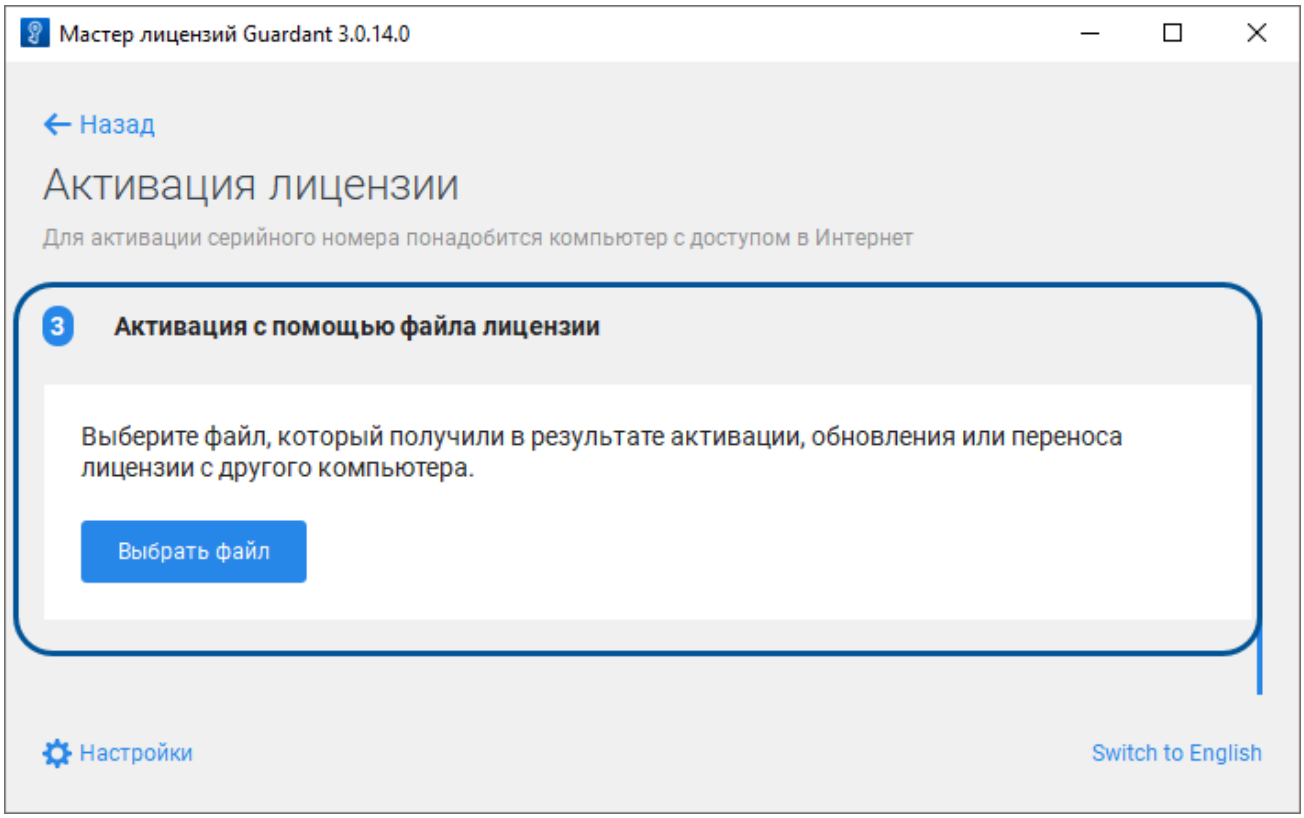


5.7. Перенесите полученный файл активации лицензии формата `*.license` на компьютер без доступа в Интернет, на котором требуется активировать лицензию.

6. На компьютере без доступа в Интернет нажмите кнопку **Продолжить, у меня есть файл лицензии**.

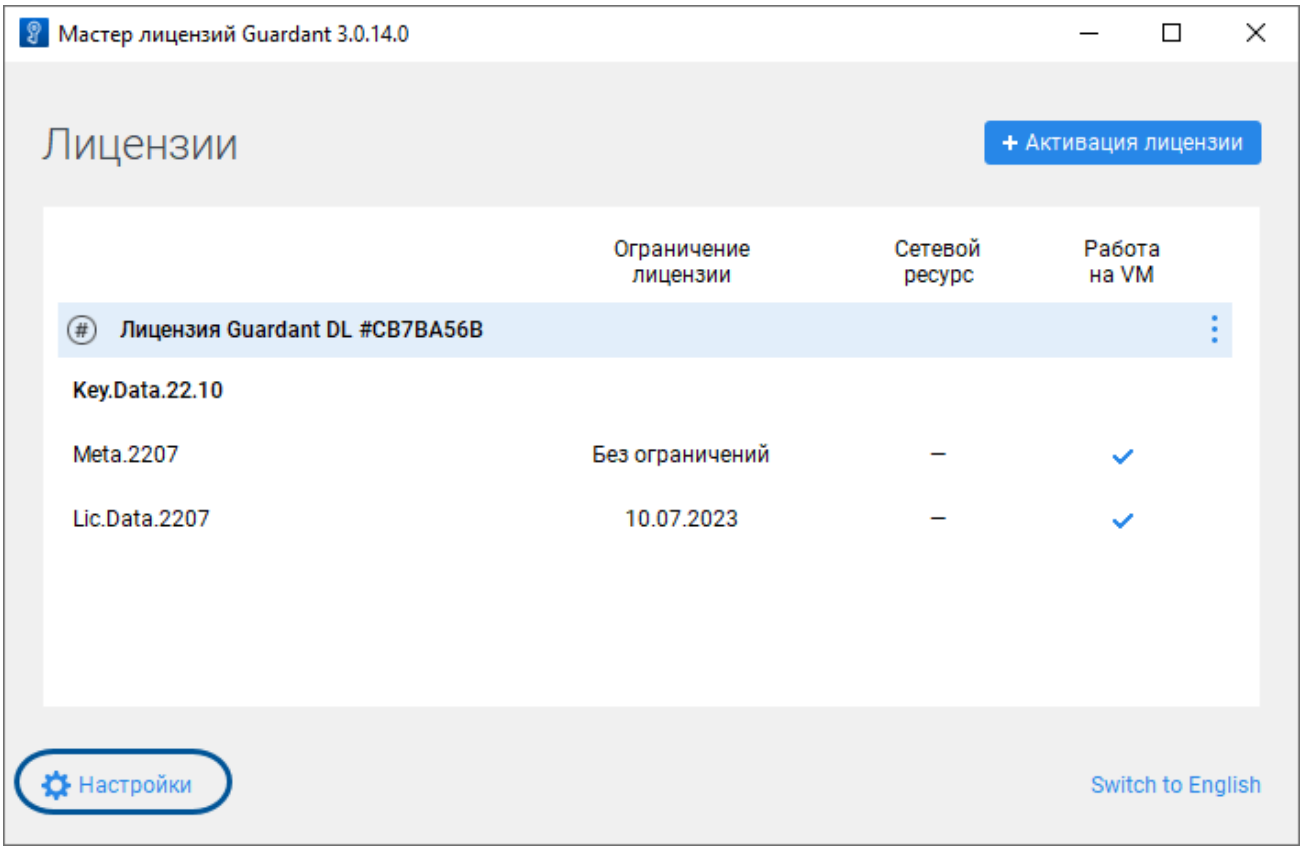


7. Нажмите кнопку **Выбрать файл** и выберите файл формата `*.license`, перенесенный с компьютера с доступом в Интернет.



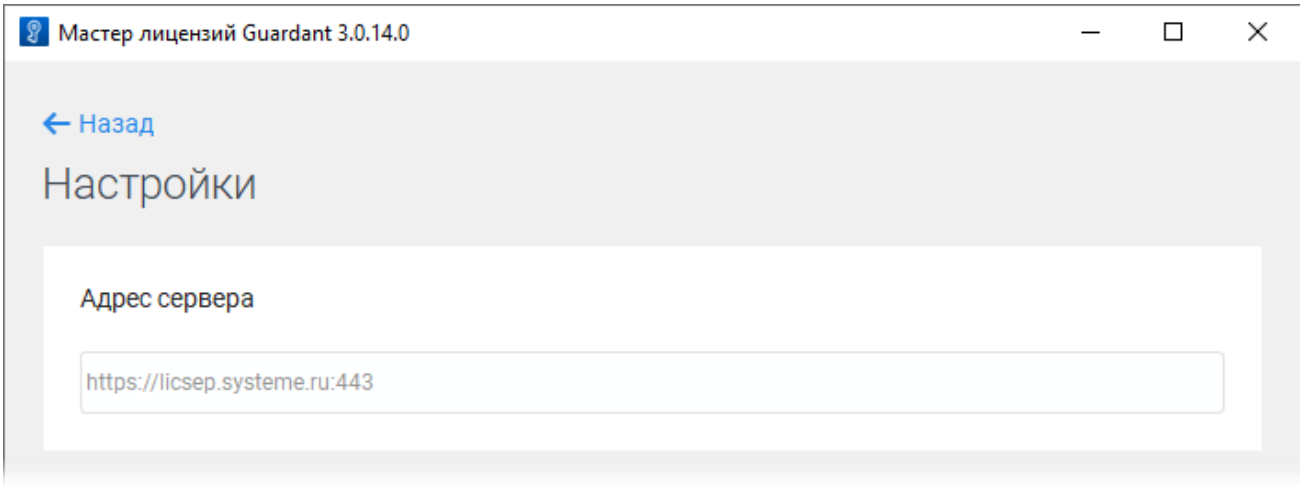
Обновление на компьютере с доступом в Интернет

1. Запустите приложение Мастер лицензий Guardant.
2. Перейдите в **Настройки**:



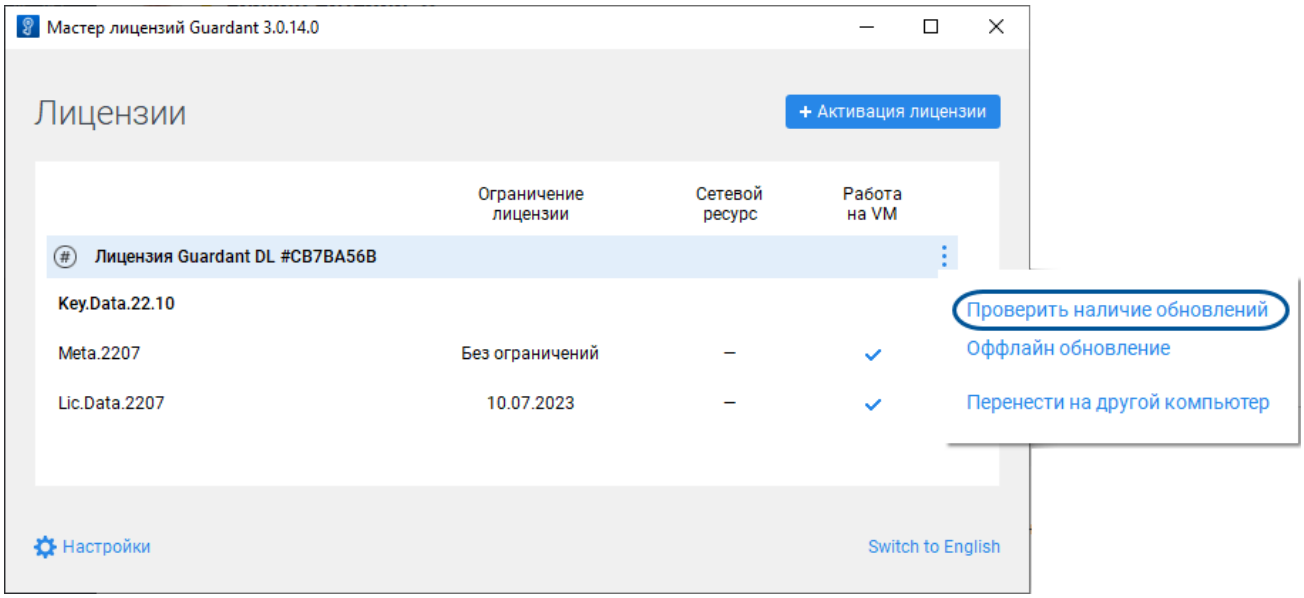
3. Укажите адрес сервера обновления лицензий.

```
https://licsep.systeme.ru:443
```



4. Вернитесь в окно **Лицензии**, нажав **Назад**.

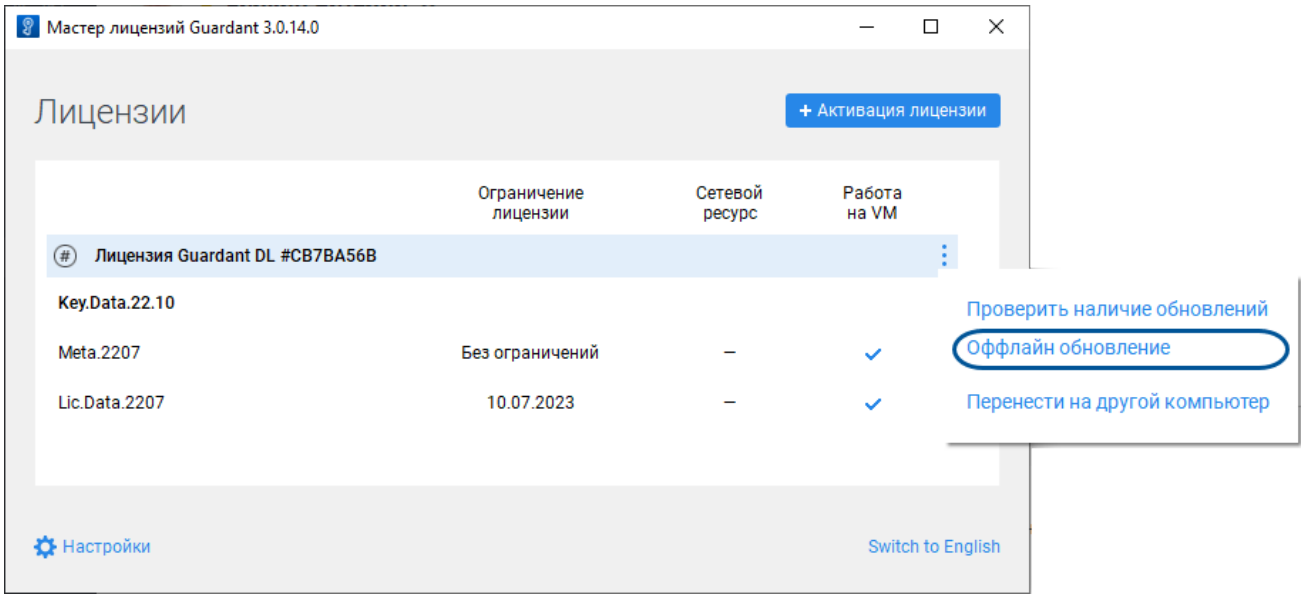
5. В окне **Лицензии** в меню ключа выберите команду **Проверить наличие обновлений**.



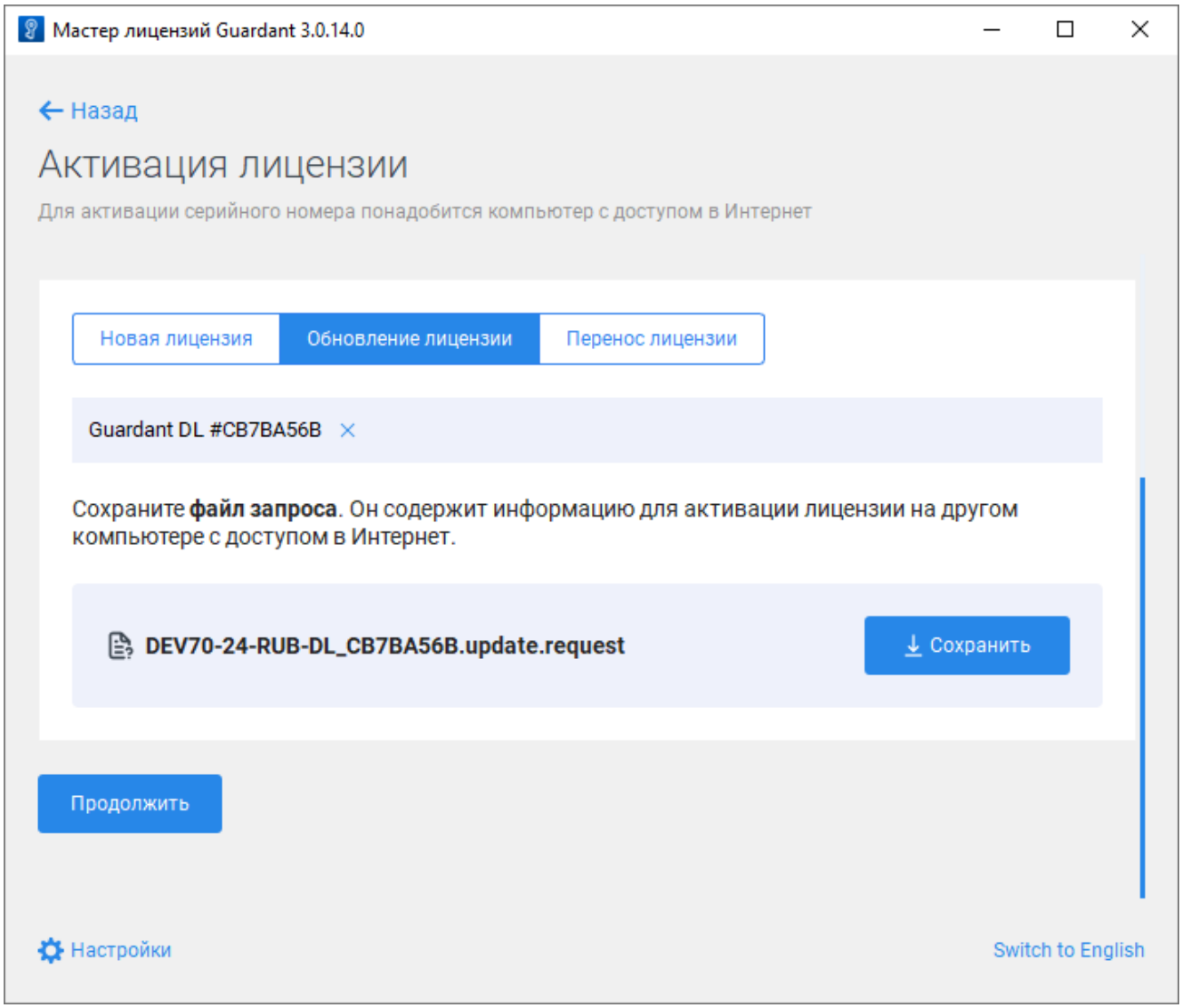
6. Если для ключа будут обнаружены обновления, то они отобразятся в списке **Обновления лицензий**. Для обновления лицензии ключа нажмите кнопку **Применить**.

Обновление на компьютере без доступа в Интернет

1. Запустите приложение Мастер лицензий Guardant.
2. В окне **Лицензии** в меню ключа выберите команду **Оффлайн обновление**.



3. На вкладке **Обновление лицензии** нажмите кнопку **Сохранить**, сохраните на диске файл запроса формата `*.request` и нажмите кнопку **Продолжить**.

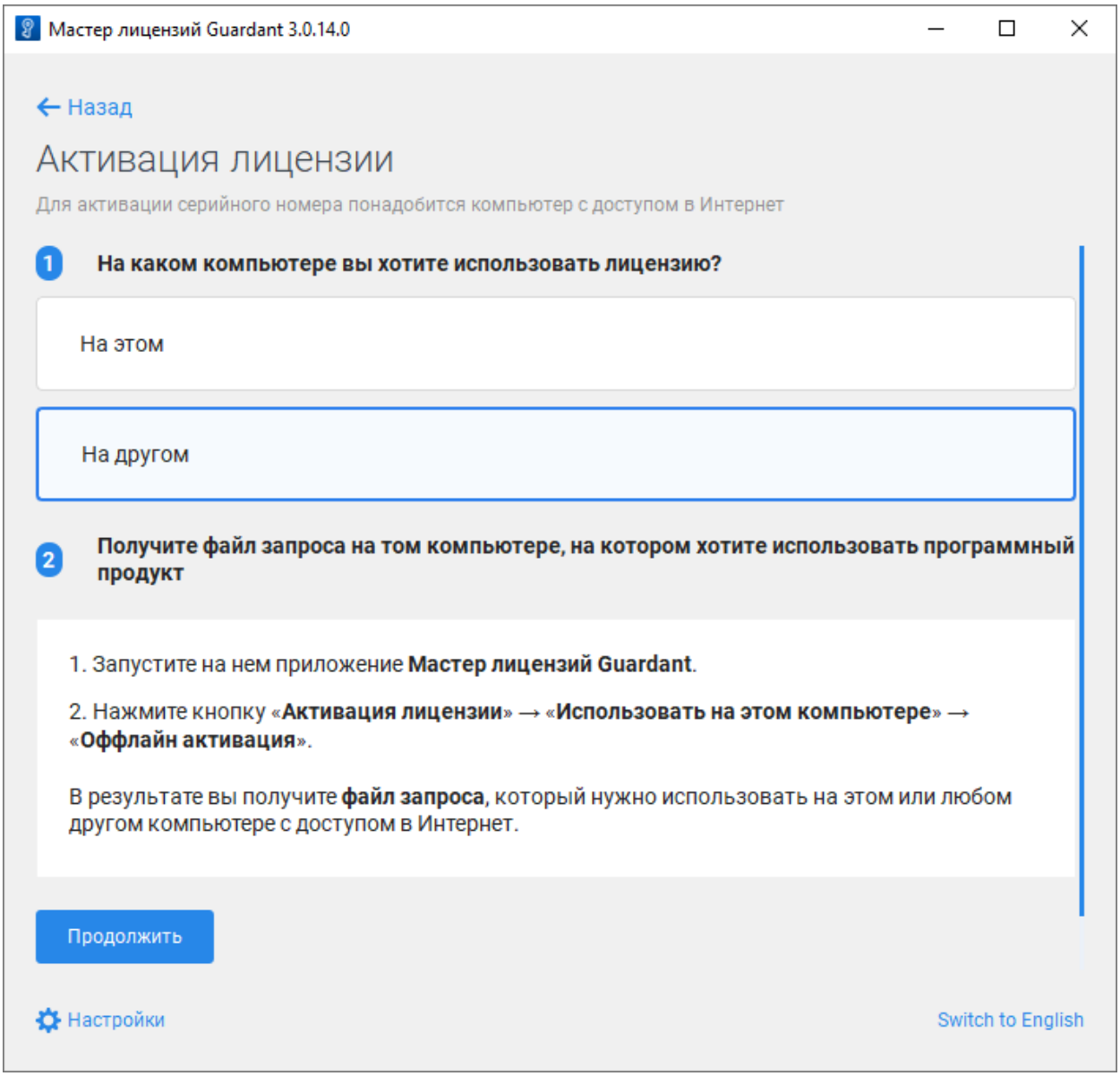


4. Перейдите на компьютер с доступом в Интернет и запустите приложение Мастер лицензий Guardant.
   4.1. Перейдите в **Настройки** и укажите адрес сервера обновления лицензий.

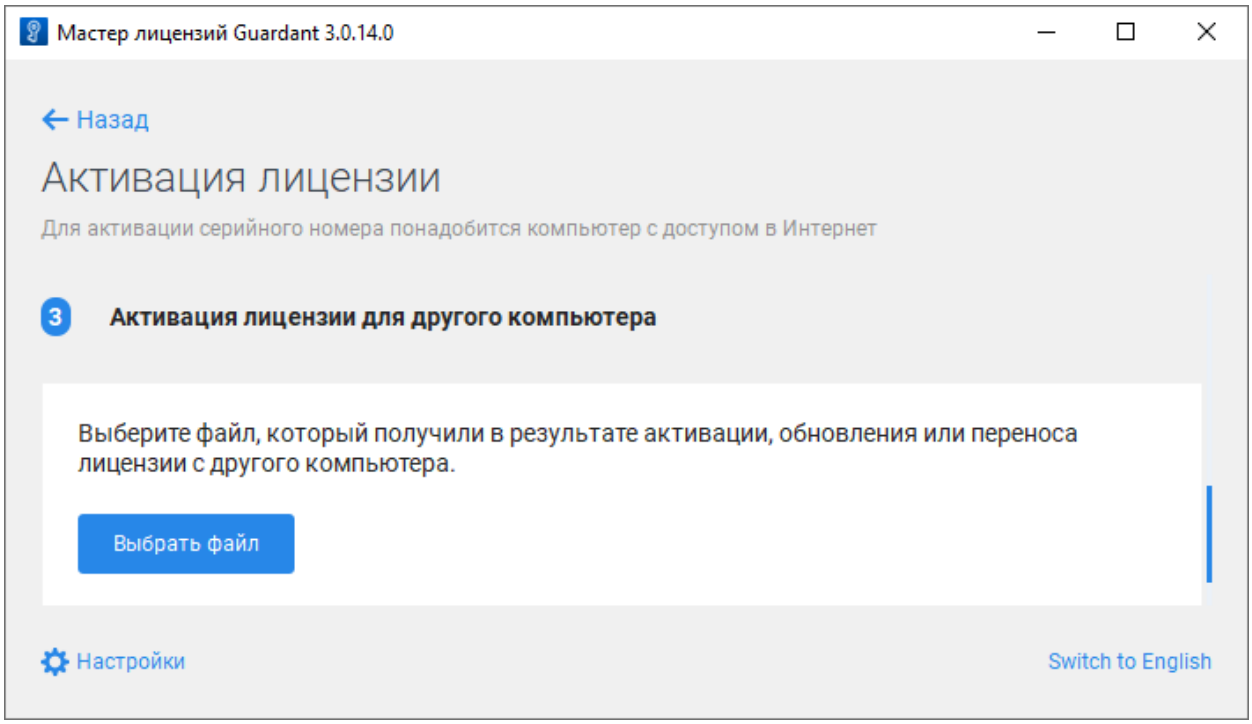
```
https://licsep.systeme.ru:443
```

   4.2. Вернитесь в окно **Лицензии** и нажмите кнопку **Активация лицензии**.

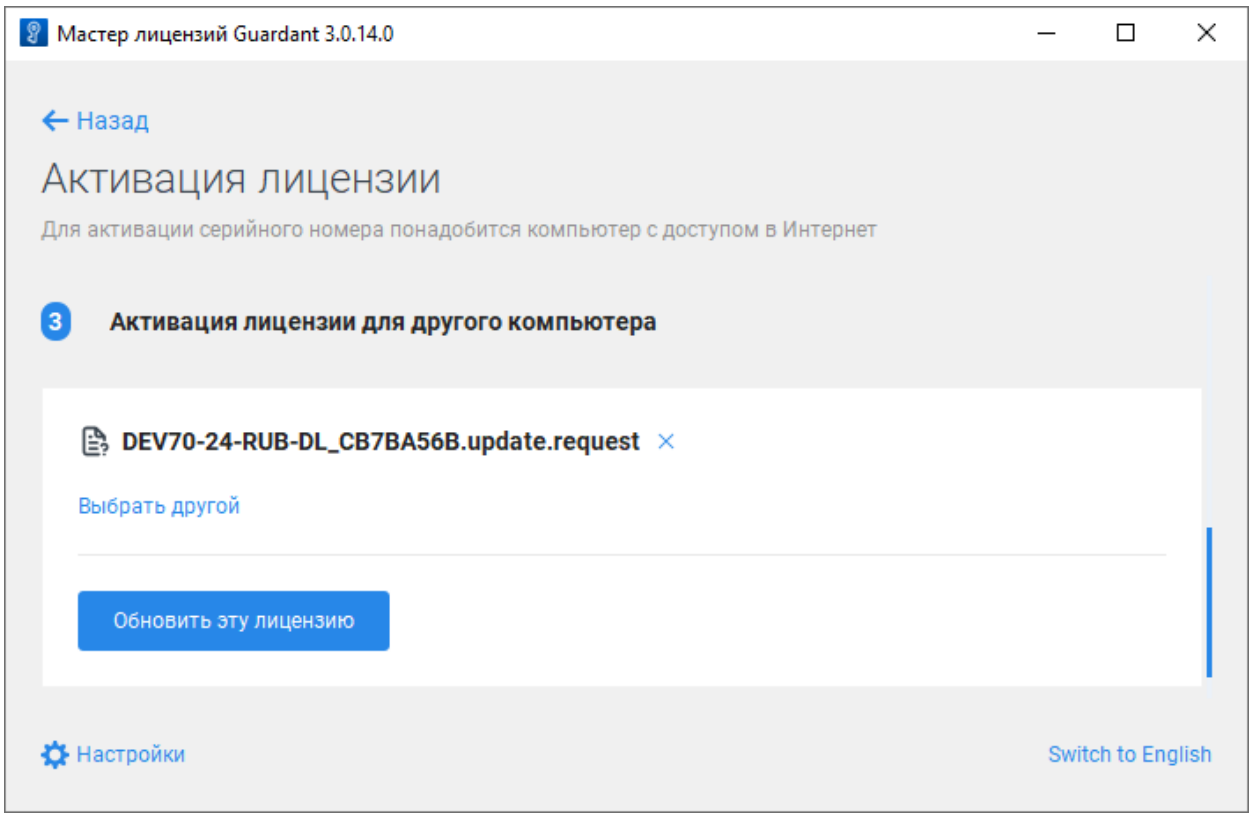
4.3. Укажите компьютер, на котором будет использоваться лицензия - **На другом** и нажмите кнопку **Продолжить**.



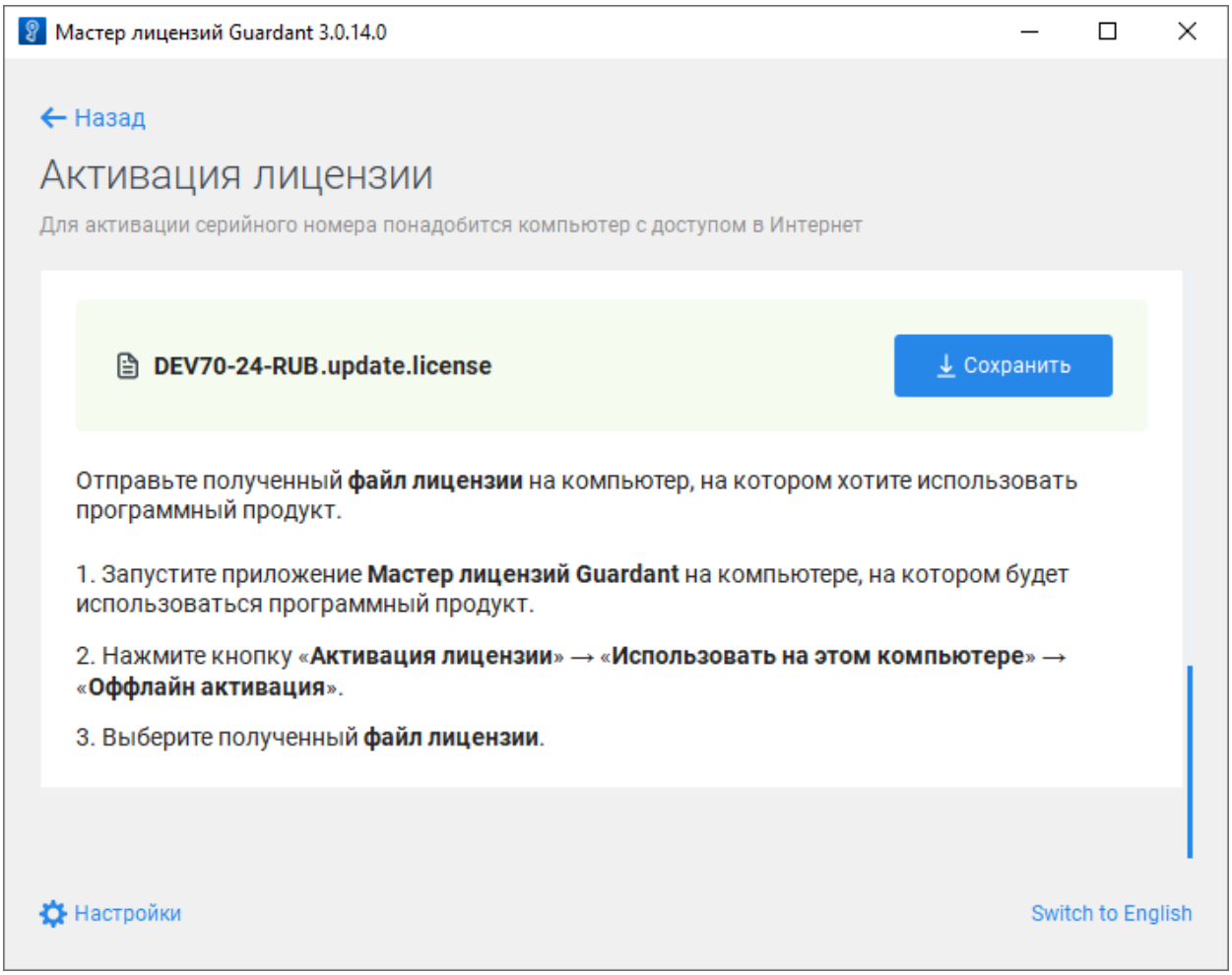
4.4. Нажмите кнопку **Выбрать файл** и выберите файл запроса формата `*.request`, перенесенный с компьютера без доступа в Интернет.



4.5. Нажмите кнопку **Обновить эту лицензию**.

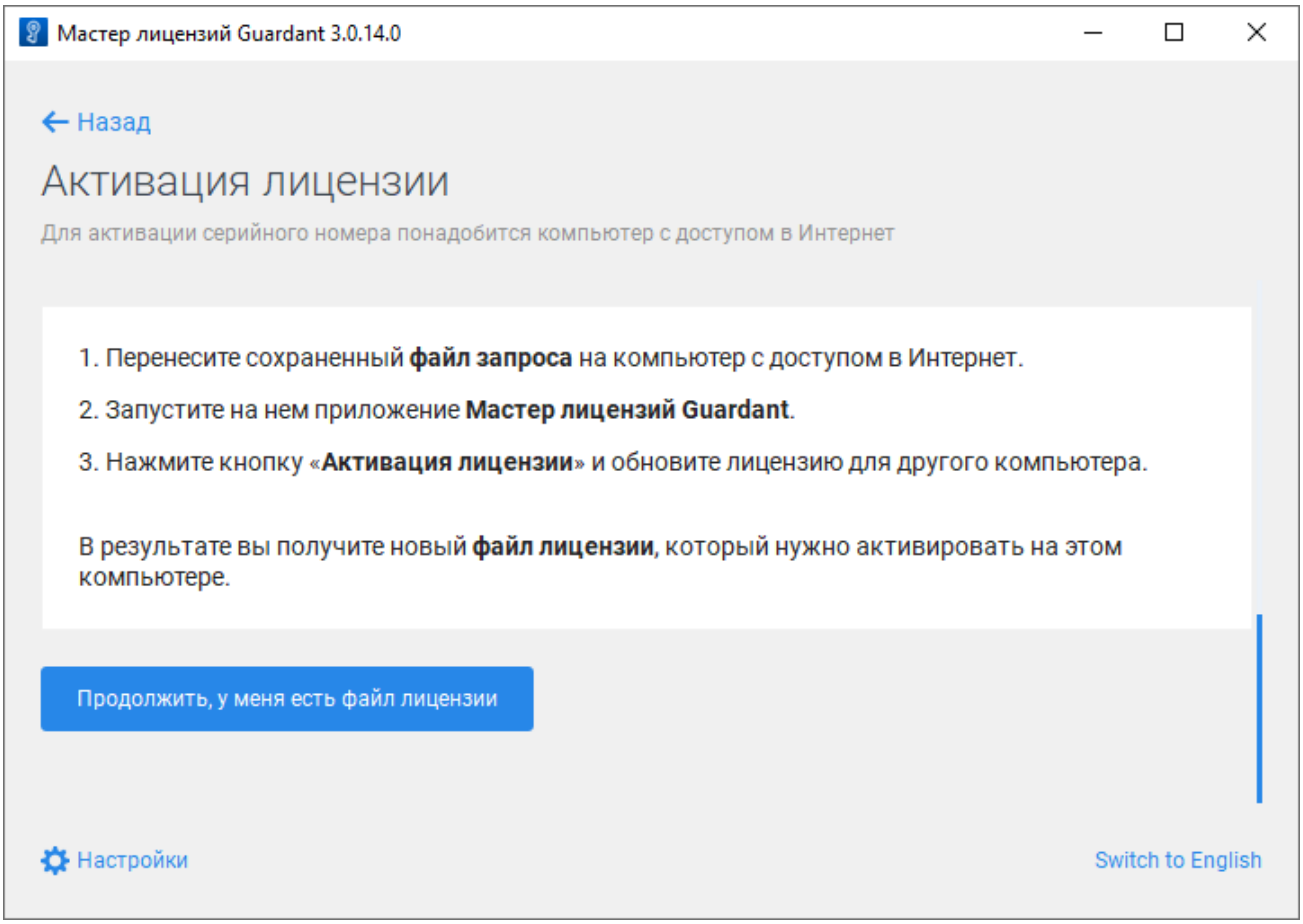


4.6. Нажмите кнопку **Сохранить** и сохраните на диске файл обновления лицензии формата `*.license`.

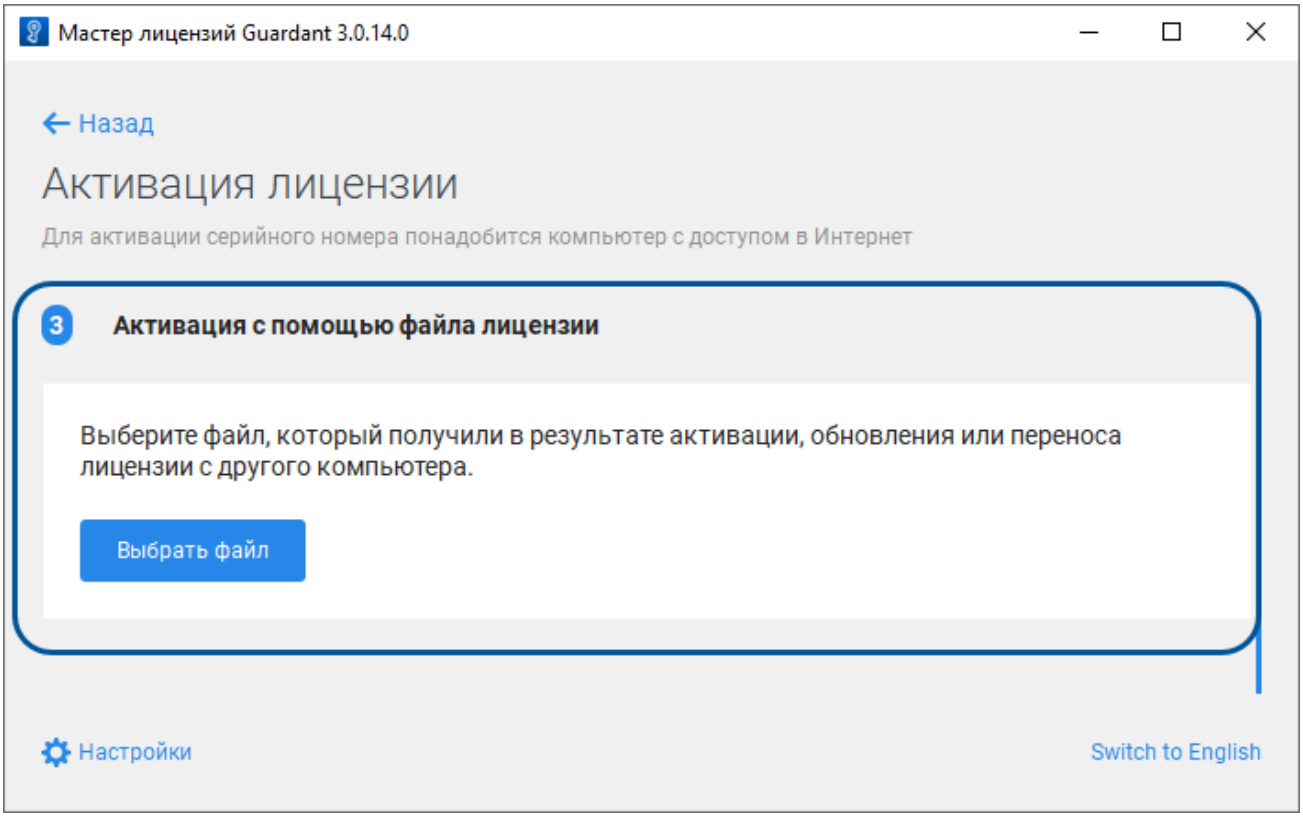


4.7. Перенесите полученный файл обновления лицензии формата `*.license` на компьютер без доступа в Интернет, на котором требуется активировать лицензию.

5. На компьютере без доступа в Интернет нажмите кнопку **Продолжить, у меня есть файл лицензии**.

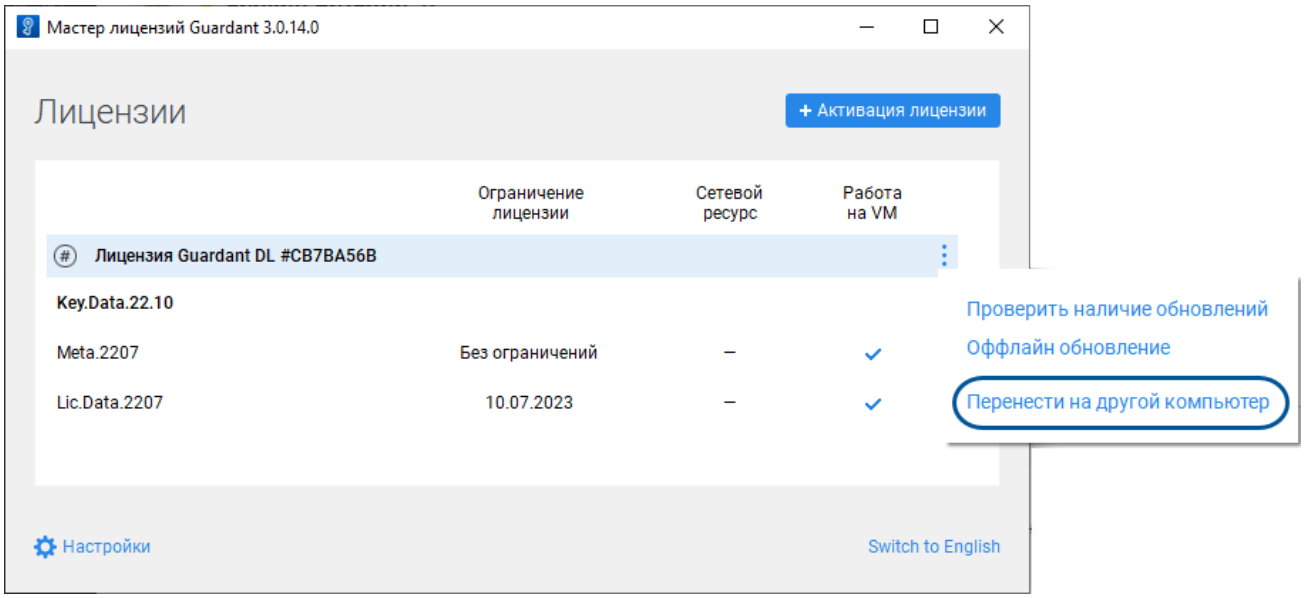


6. Нажмите кнопку **Выбрать файл** и выберите файл формата `*.license`, перенесенный с компьютера с доступом в Интернет.

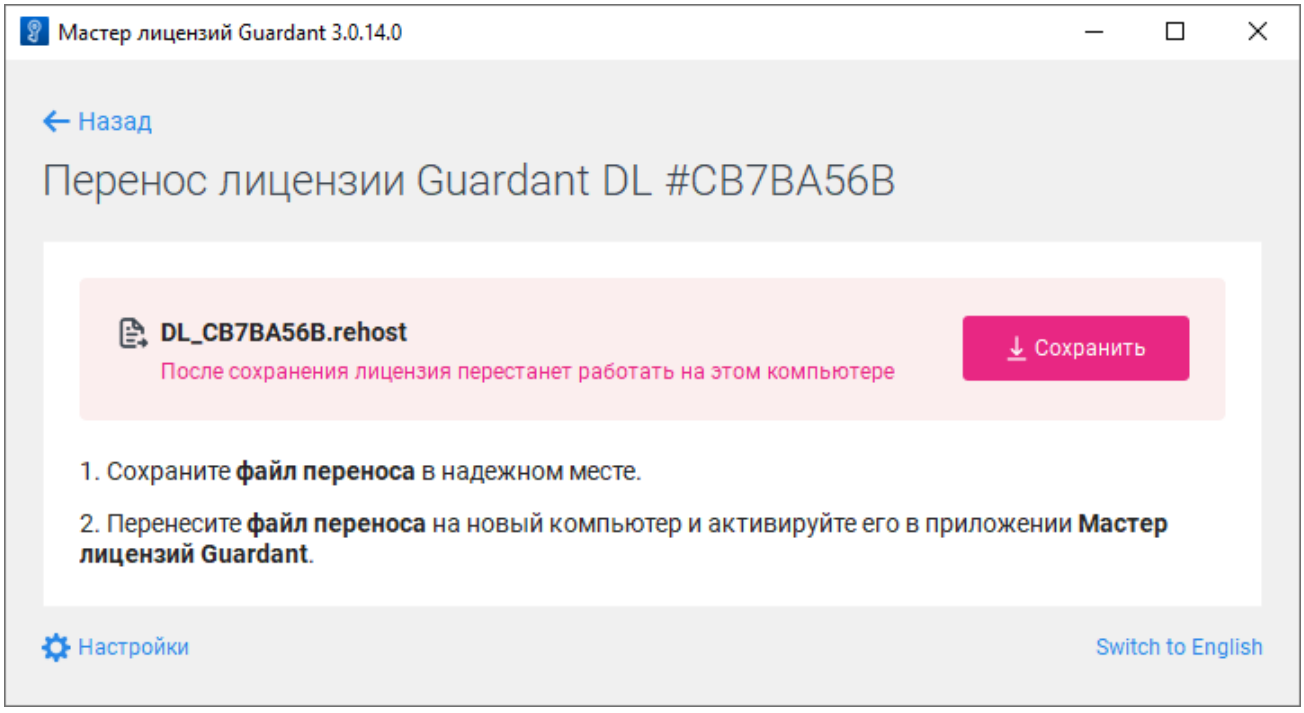


Перенос на другой компьютер

1. Запустите приложение Мастер лицензий Guardant.
2. В окне **Лицензии** в меню ключа выберите команду **Перенести на другой компьютер**.

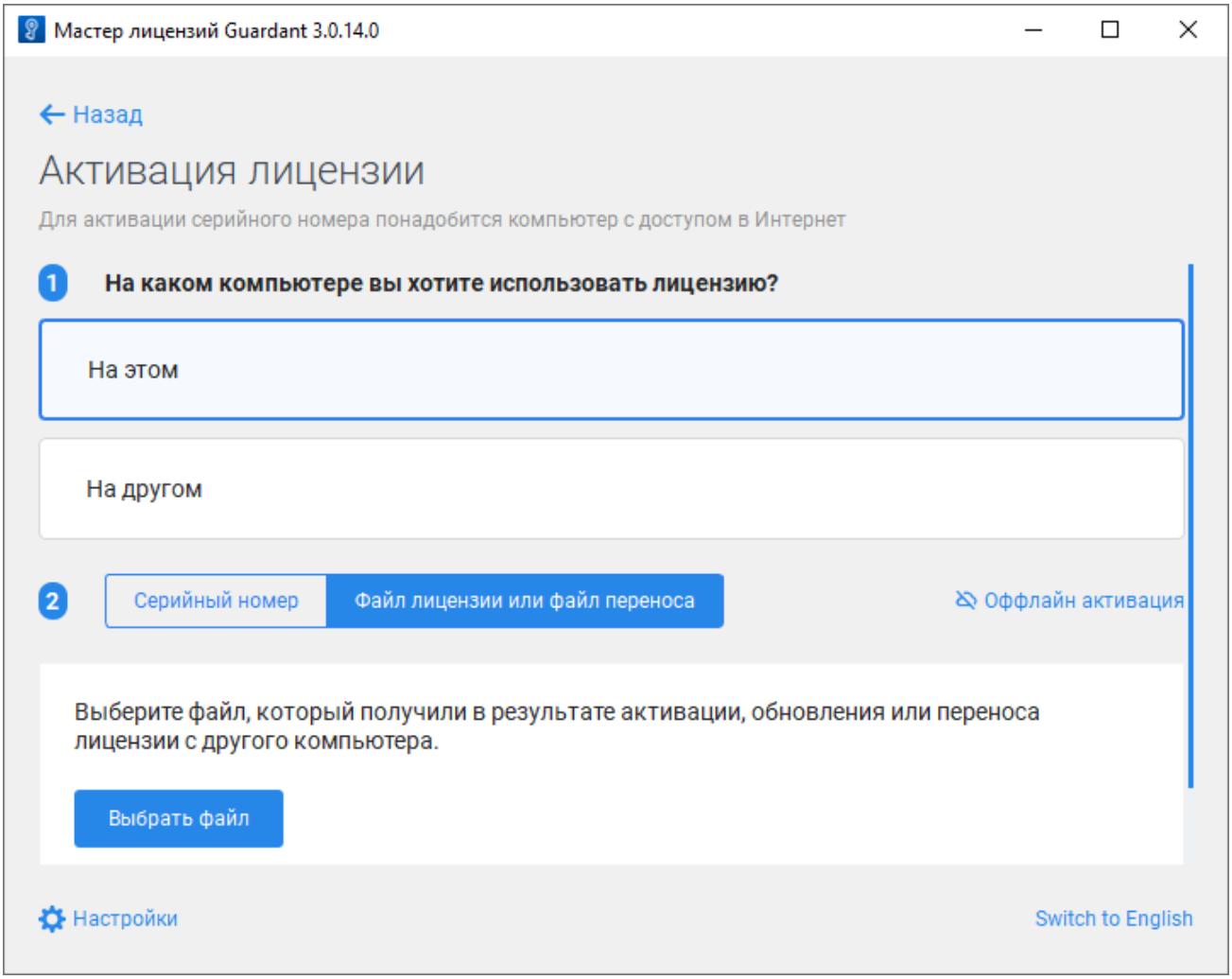


3. В окне **Перенос лицензии Guardant DL** нажмите кнопку **Сохранить** и сохраните на диске файл переноса формата `*.rehost`.



4. На другом компьютере запустите приложение Мастер лицензий Guardant и нажмите кнопку **Активация лицензии**.

5. Укажите компьютер, на котором будет использоваться лицензия - **На этом**, перейдите на вкладку **Файл лицензии или файл переноса**, нажмите кнопку **Выбрать файл** и выберите ранее сохраненный файл переноса формата `*.rehost`.



16.1.2. ОС Linux

Для лицензирования компонентов Систэм Платформ, установленных на компьютере с ОС Linux:

- установите сервер лицензирования SePlatform.License Server;
- установите Guardant Control Center.

16.1.2.1. Установка SePlatform.License Server

ОБРАТИТЕ ВНИМАНИЕ

Команда установки выполняется только от суперпользователя **«root»**.

Имя устанавливаемого пакета: `seplatform.licenseserver.agent-x.x.x+xx.xxxxx.deb` или `seplatform.licenseserver.agent-x.x.x+xx.xxxxx.rpm` в зависимости от используемой ОС Linux. Находясь в папке с установочным пакетом, запустите установку штатным пакетным менеджером.
Установка пакета `*.rpm` с помощью пакетного менеджера YUM:

```
yum install seplatform.licensing.agent-x.x.x+xx.xxxxx.rpm
```

Установка пакета `*.rpm` с помощью пакетного менеджера RPM:

```
rpm -i seplatform.licensing.agent-x.x.x+xx.xxxxx.rpm
```

Установка пакета `*.deb` с помощью пакетного менеджера apt:

```
apt-get install seplatform.licensing.agent-x.x.x+xx.xxxxx.deb
```

Установка пакета `*.deb` с помощью пакетного менеджера dpkg:

```
sudo dpkg -i seplatform.licensing.agent-x.x.x+xx.xxxxx.deb
```

16.1.2.2. Установка Guardant Control Center

Установите Guardant Control Center (установочные пакеты расположены в папке `\Сторонние компоненты\Guardant\x.xx\control`).

ОБРАТИТЕ ВНИМАНИЕ

Команда установки выполняется только от суперпользователя **«root»**.

Находясь в папке с установочным пакетом, запустите установку штатным пакетным менеджером.
Установка пакета `*.rpm` с помощью пакетного менеджера YUM:

```
yum install grdcontrol-x.x-xxxx.rpm
```

Установка пакета `*.rpm` с помощью пакетного менеджера RPM:

```
rpm -i grdcontrol-x.x-xxxx.rpm
```

Установка пакета `*.deb` с помощью пакетного менеджера apt:

```
apt-get install grdcontrol-x.x_xxxx.deb
```

Установка пакета `*.deb` с помощью пакетного менеджера dpkg:

```
sudo dpkg -i grdcontrol-x.x_xxxx.deb
```

16.1.2.3. Аппаратный ключ Guardant Sign

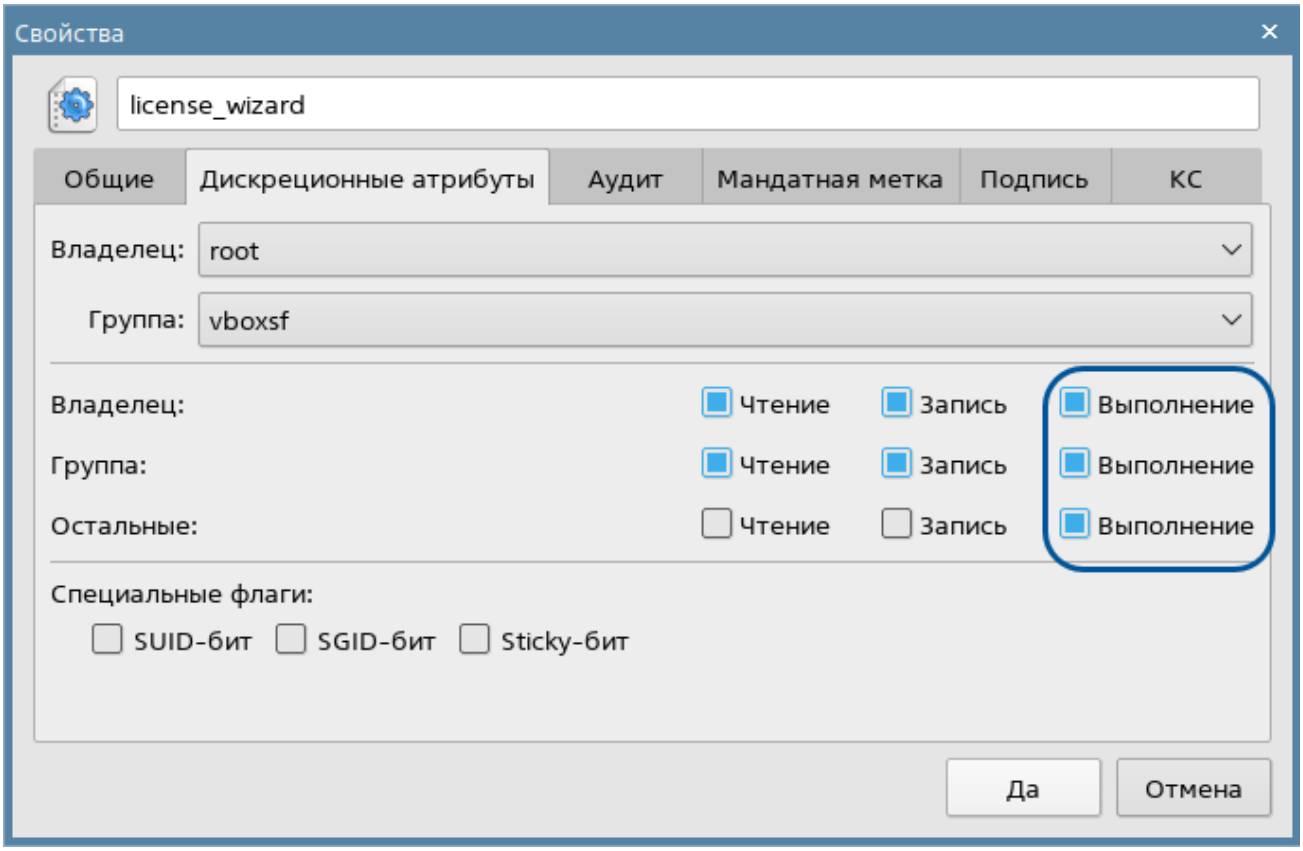
Подключите аппаратный ключ Guardant Sign в USB разъем компьютера. Дополнительных действий не требуется. Ключ готов к работе.

Обновление

ОБРАТИТЕ ВНИМАНИЕ

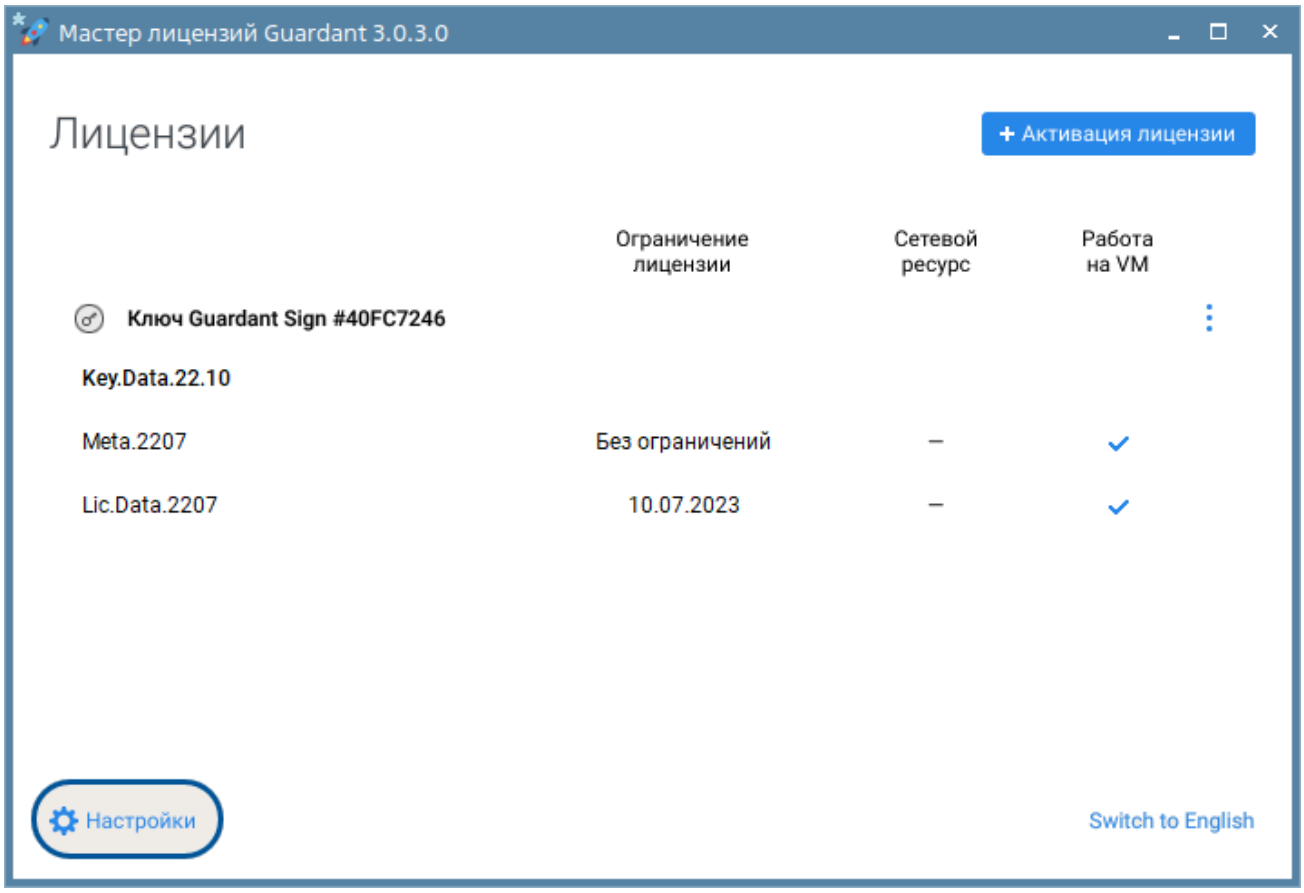
Для обновления состава лицензии аппаратного ключа Guardant Sign требуется подключение к сети Интернет.

1. Исполняемому файлу `license_wizard` в свойствах установите права на запуск (расположен в папке `\Сторонние компоненты\Guardant\x.xx\license_activation`).



2. Запустите Мастер лицензий Guardant - исполняемый файл `license_wizard`.

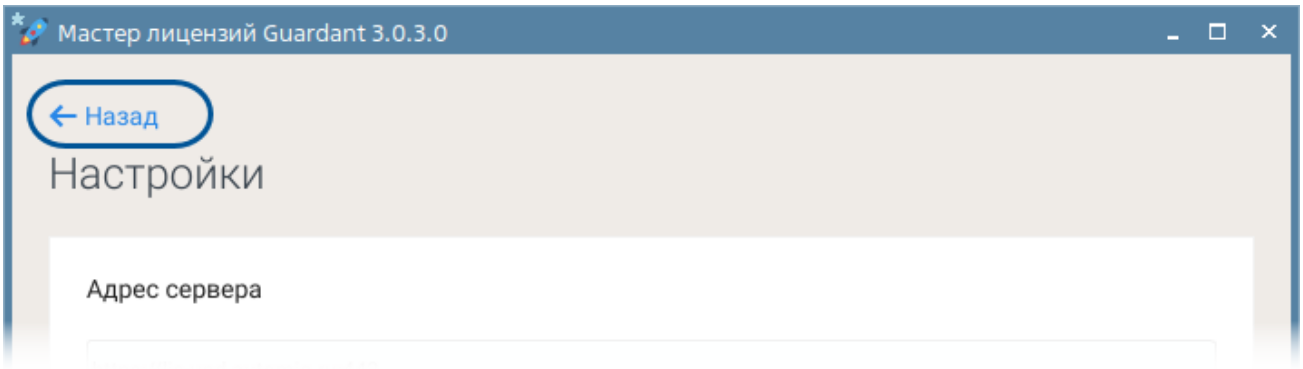
3. Перейдите в **Настройки**:



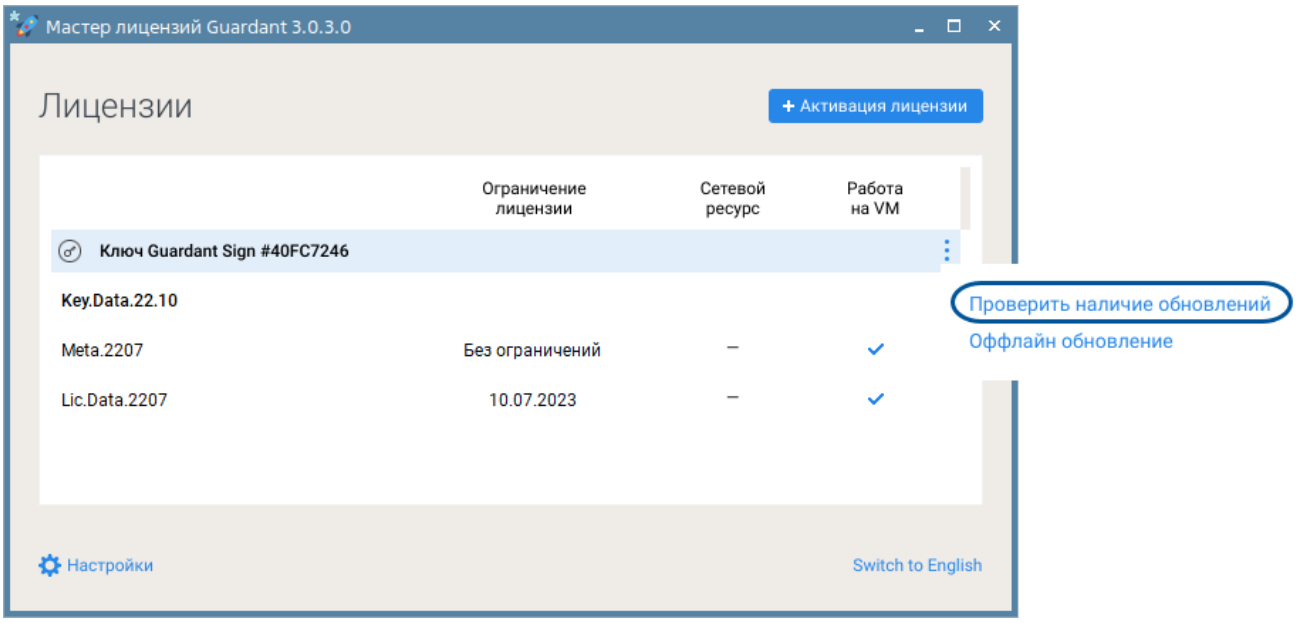
4. Укажите адрес сервера обновления лицензий:

```
https://licsep.systeme.ru:443
```

5. Вернитесь в окно **Лицензии**, нажав **Назад**.



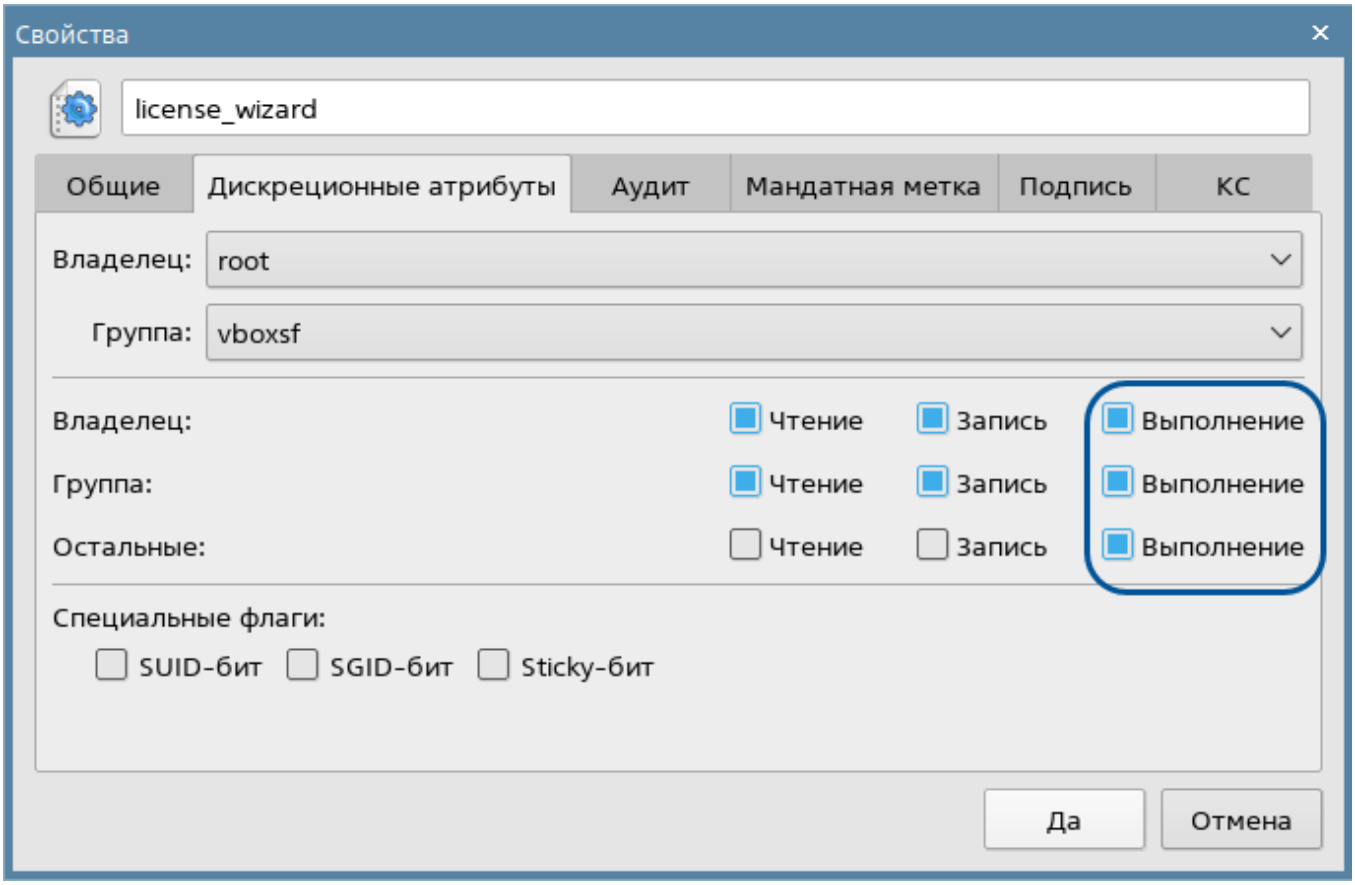
6. В меню ключа выберите команду **Проверить наличие обновлений**.



7. Если для ключа будут обнаружены обновления, то они отобразятся в списке **Обновления лицензий**. Для обновления лицензии ключа нажмите кнопку **Применить**.

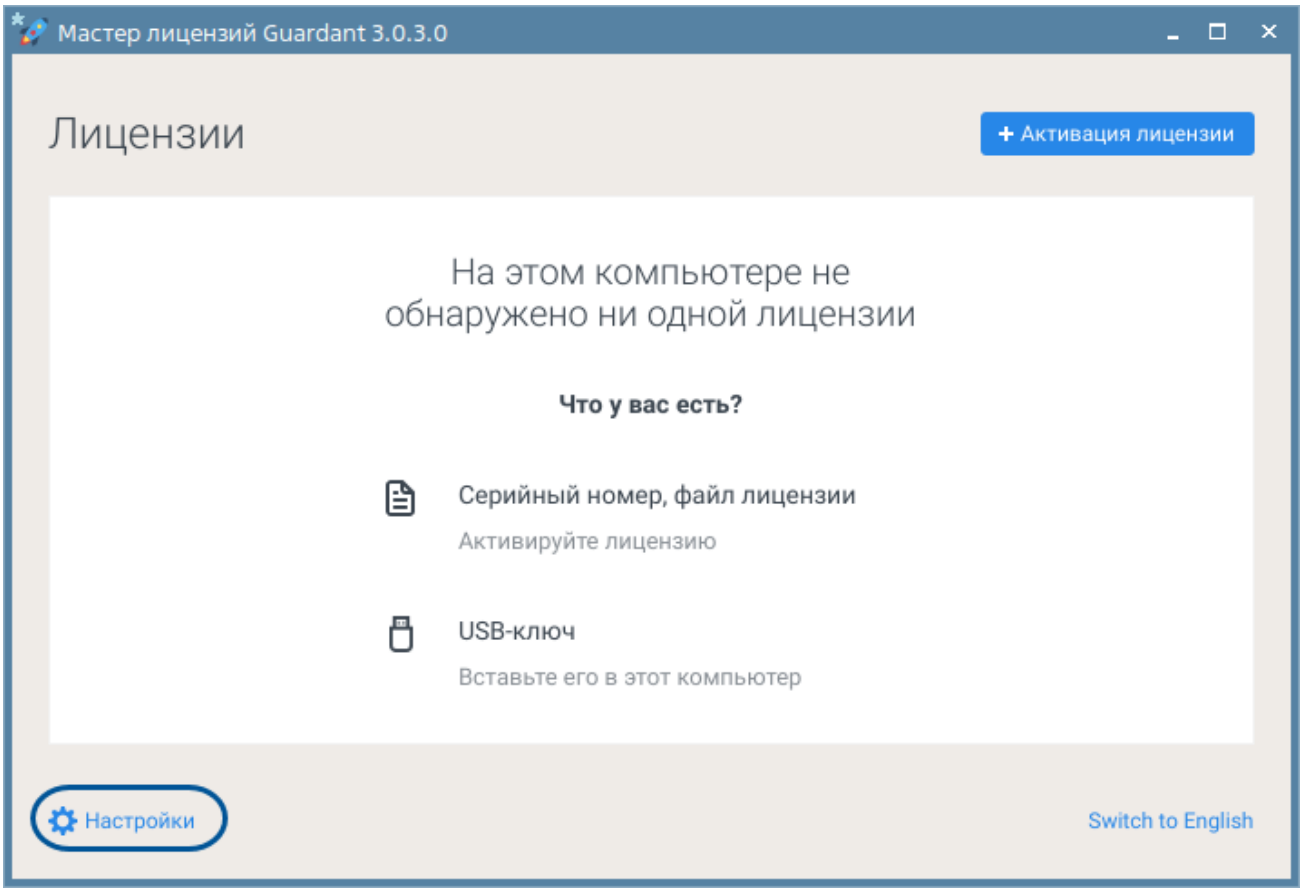
16.1.2.4. Программный ключ Guardant DL

Активация, обновление и перенос лицензии программного ключа Guardant DL выполняется в Мастере лицензий Guardant - исполняемый файл `license_wizard` (расположен в папке `\Сторонние компоненты\Guardant\x.xx\license_activation`). В свойствах `license_wizard` установите права на запуск.


Свойства
license_wizard
Общие
Дискреционные атрибуты
Аудит
Мандатная метка
Подпись
КС
Владелец:
root
Группа:
vboxsf
Владелец:
Чтение
Запись
Выполнение
Группа:
Чтение
Запись
Выполнение
Остальные:
Чтение
Запись
Выполнение
Специальные флаги:
SUID-бит
SGID-бит
Sticky-бит
Да
Отмена

Активация на компьютере с доступом в Интернет

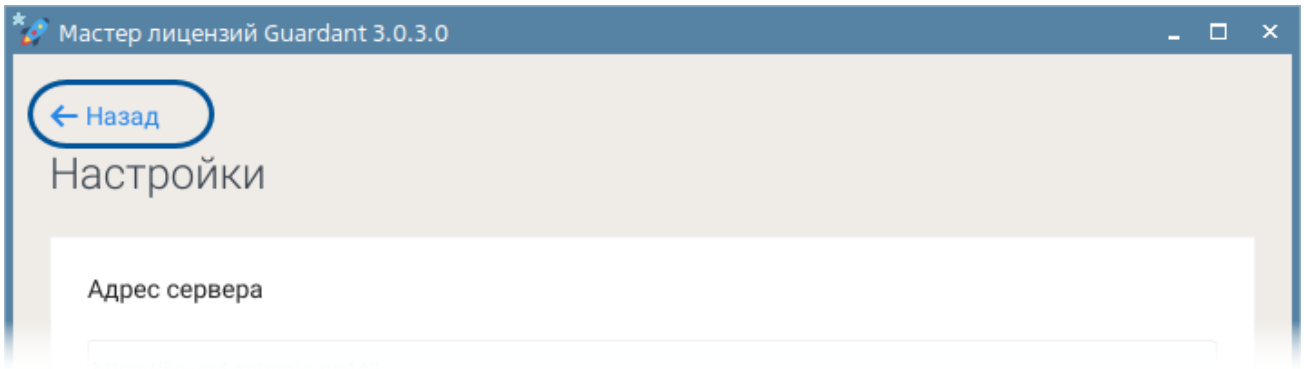
1. Запустите Мастер лицензий Guardant.
2. Перейдите в **Настройки**:



3. Укажите адрес сервера обновления лицензий:

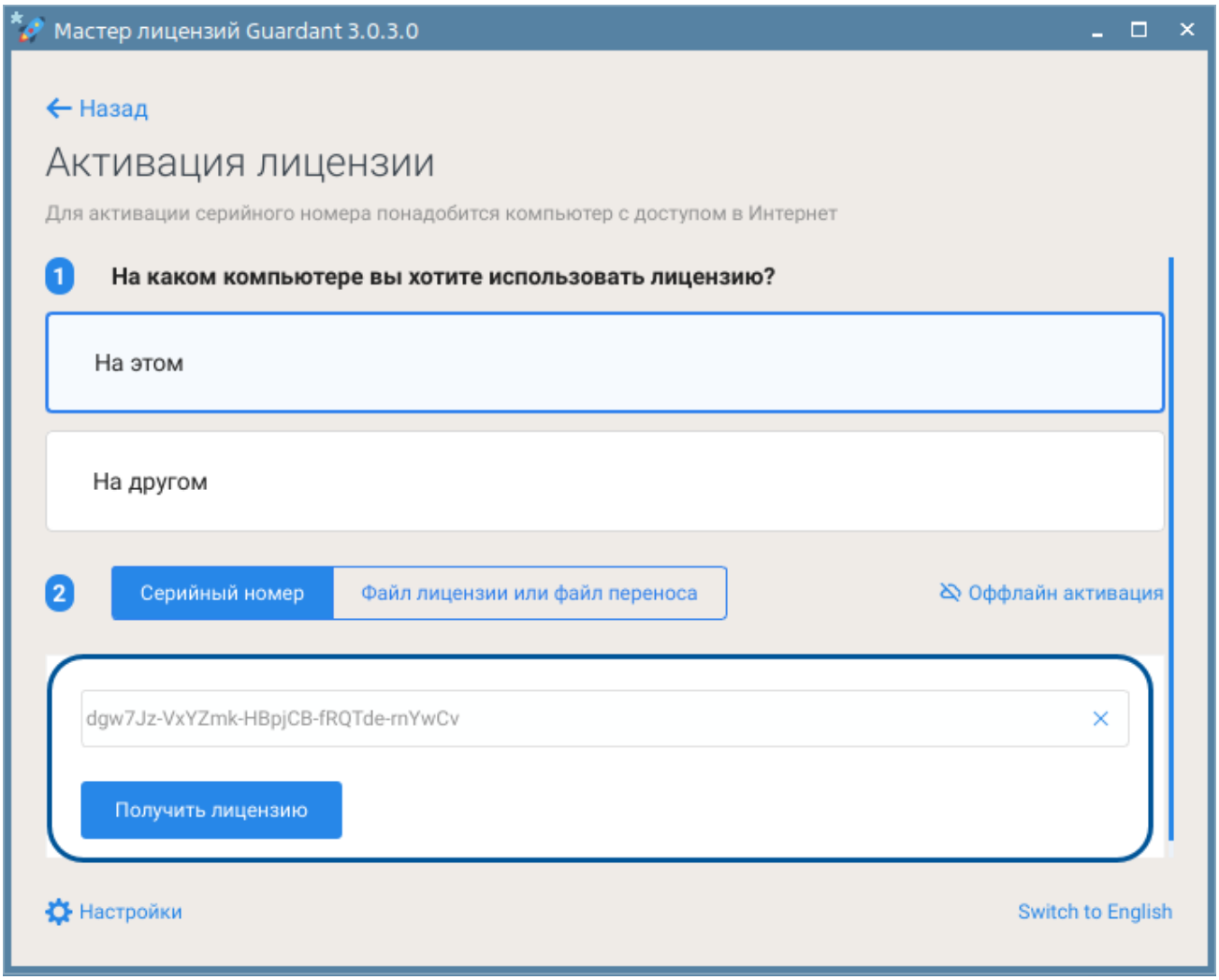
```
https://licsep.systeme.ru:443
```

4. Вернитесь в окно **Лицензии**, нажав **Назад**.



5. В окне **Лицензии** нажмите **Активация лицензии**.

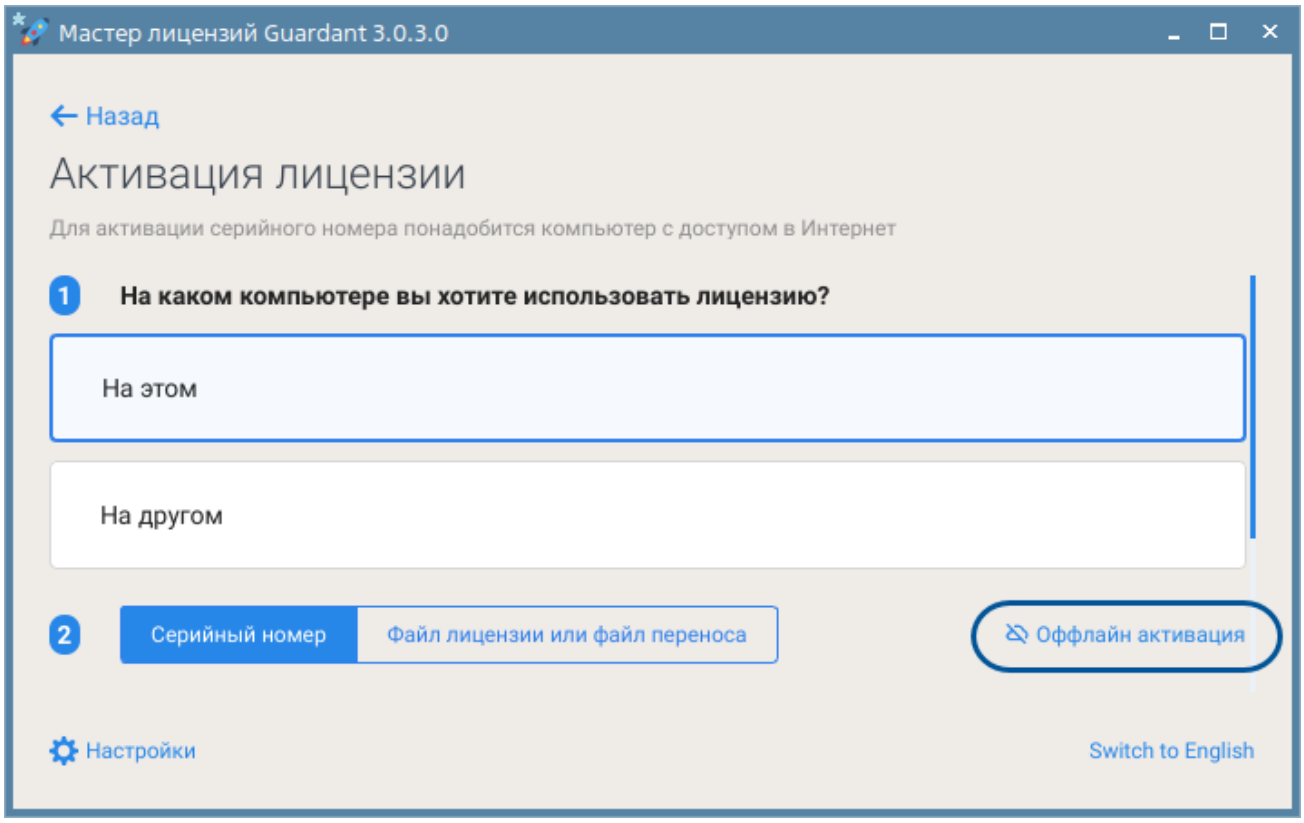
6. В окне **Активация лицензии** выберите компьютер, на котором будет использоваться лицензия - **На этом**, введите в поле ввода серийный номер программного ключа, указанный в сертификате, и нажмите кнопку **Получить лицензию**.



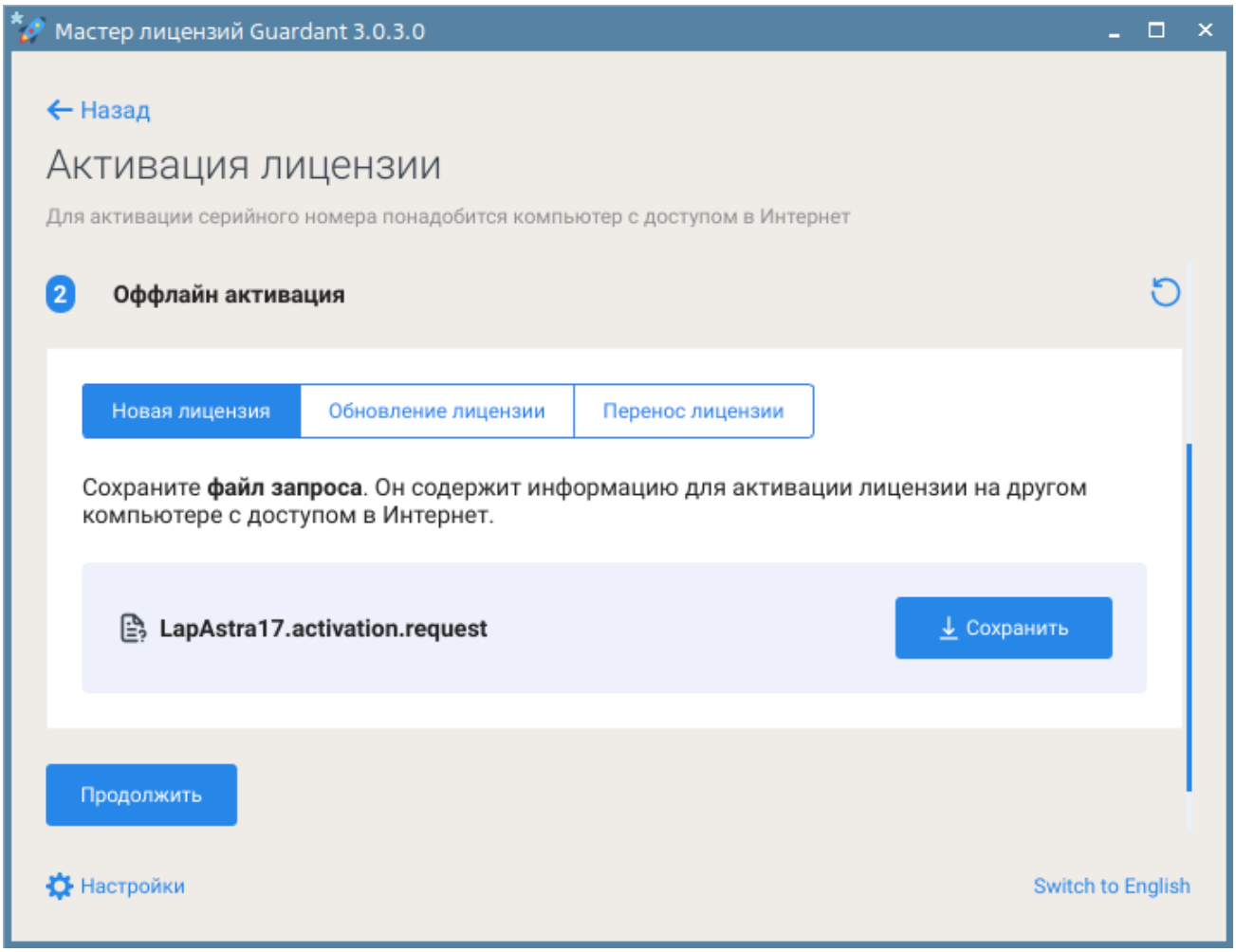
Активация на компьютере без доступа в Интернет

1. Запустите Мастер лицензий Guardant.
2. Нажмите **Активация лицензии**.

3. В окне **Активация лицензии** выберите компьютер, на котором будет использоваться лицензия - **На этом** и нажмите **Оффлайн активация**.



4. На вкладке **Новая лицензия** нажмите кнопку **Сохранить**, сохраните на диске файл запроса формата `*.request` и нажмите кнопку **Продолжить**.

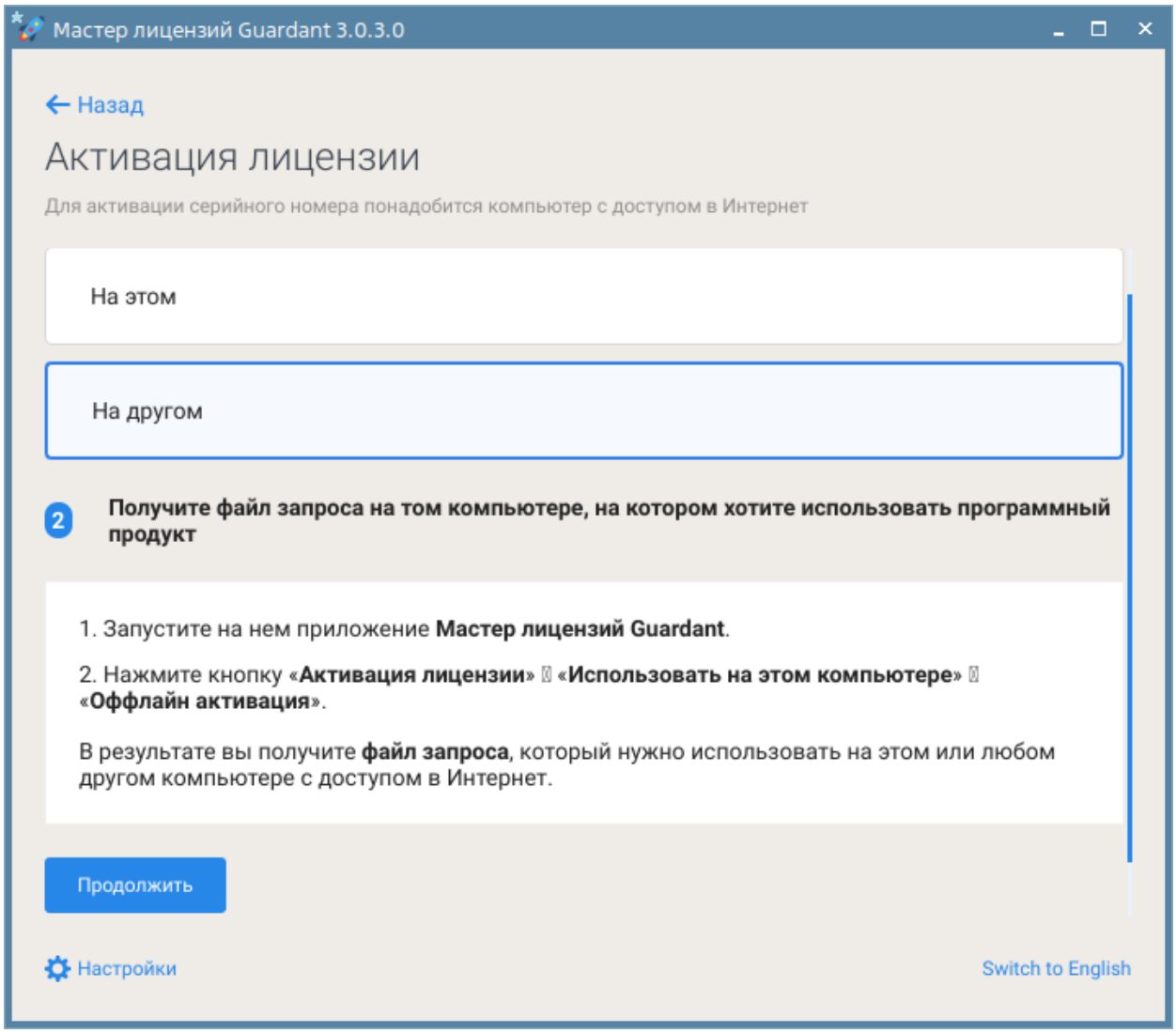


5. Перейдите на компьютер с доступом в Интернет и запустите Мастер лицензий Guardant.
   5.1. Перейдите в **Настройки** и укажите адрес сервера обновления лицензий.

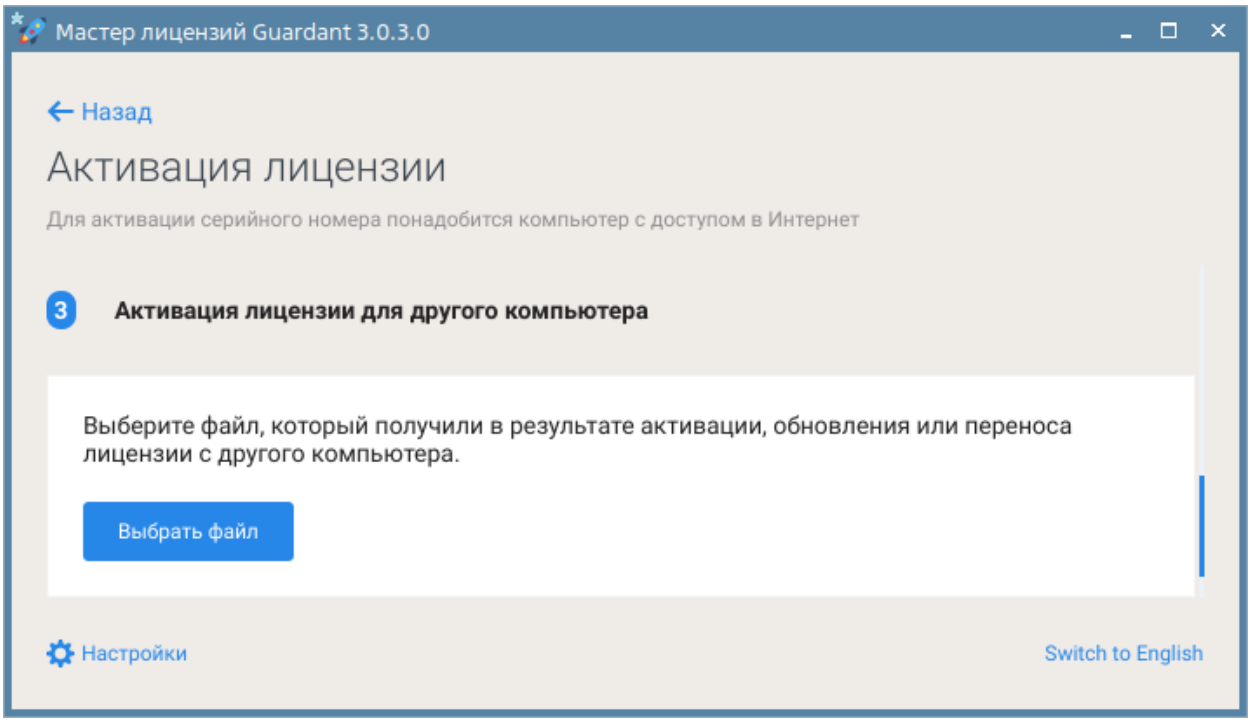
```
https://licsep.systeme.ru:443
```

   5.2. Вернитесь в окно **Лицензии** и нажмите кнопку **Активация лицензии**.

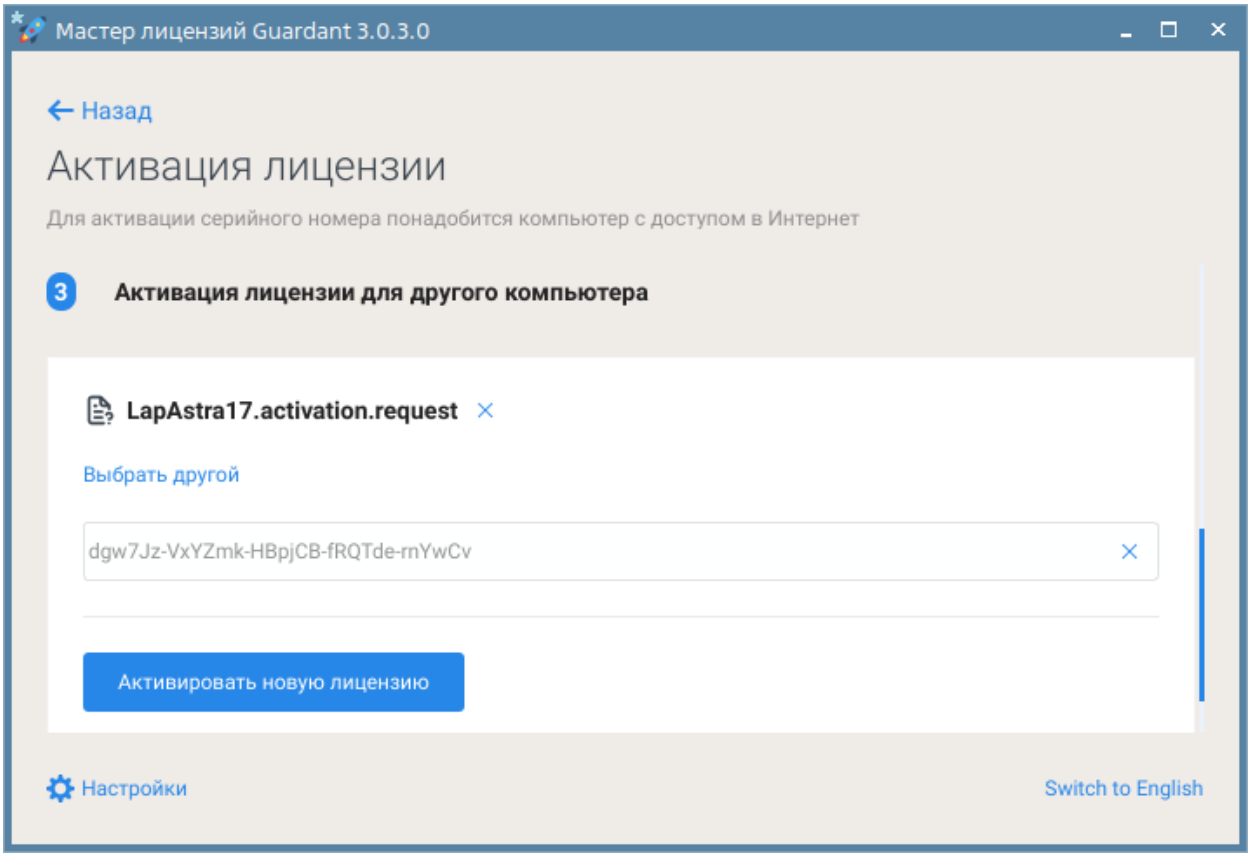
5.3. Укажите компьютер, на котором будет использоваться лицензия - **На другом** и нажмите кнопку **Продолжить**.



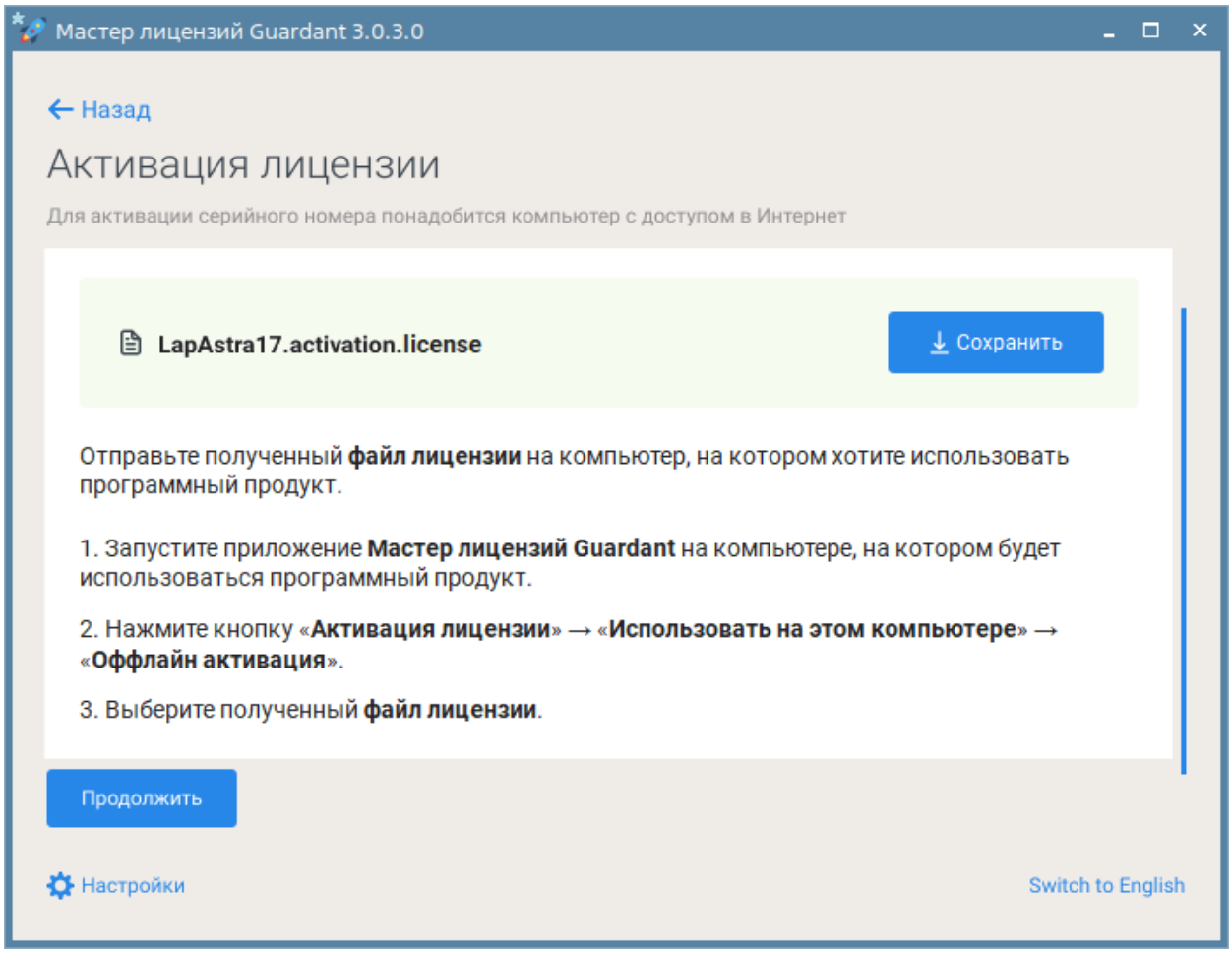
5.4. Нажмите кнопку **Выбрать файл** и выберите файл формата `*.request`, перенесенный с компьютера без доступа в Интернет.



5.5. Введите в поле ввода серийный номер программного ключа, указанный в сертификате, и нажмите кнопку **Активировать новую лицензию**.

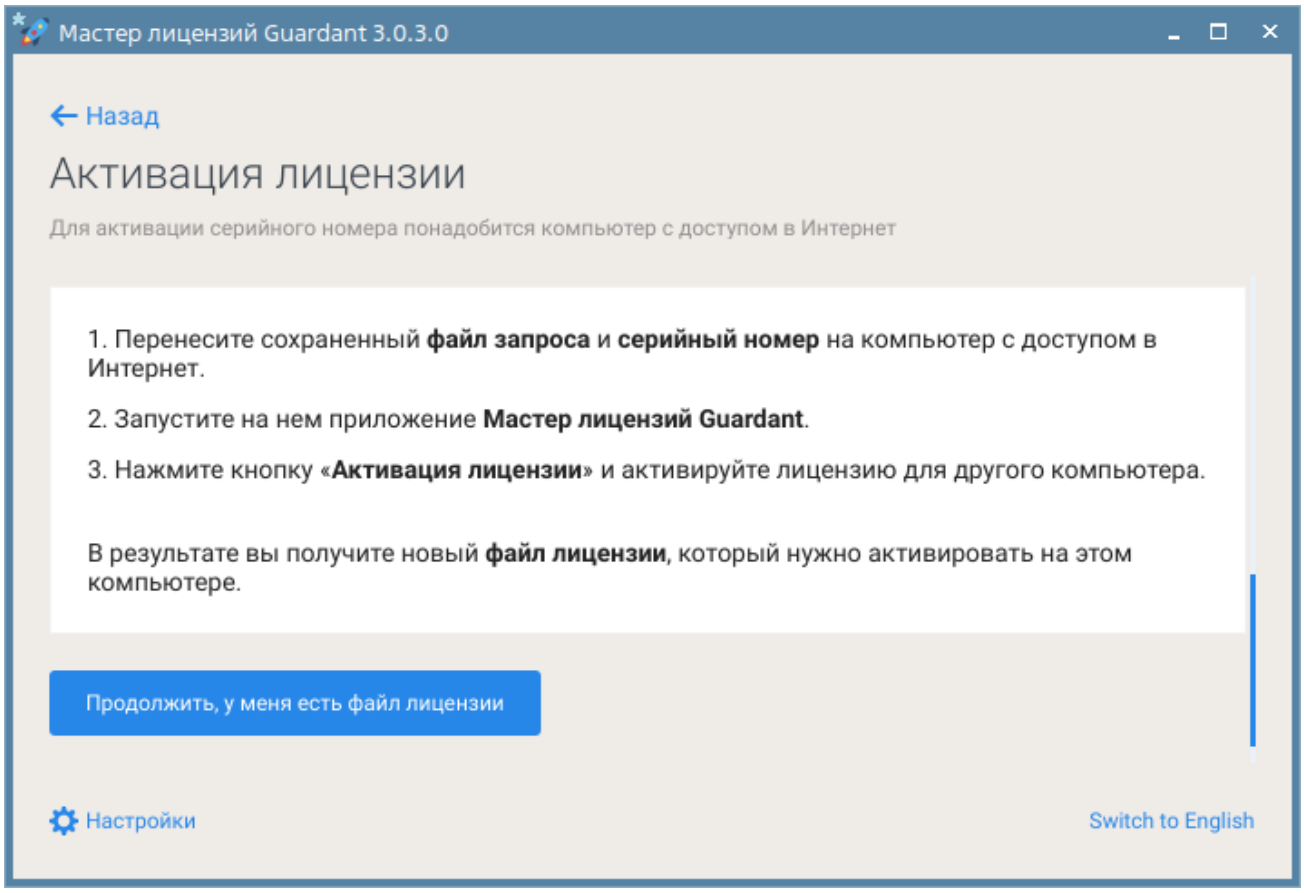


5.6. Нажмите кнопку **Сохранить** и сохраните на диске файл активации лицензии формата `*.license`.

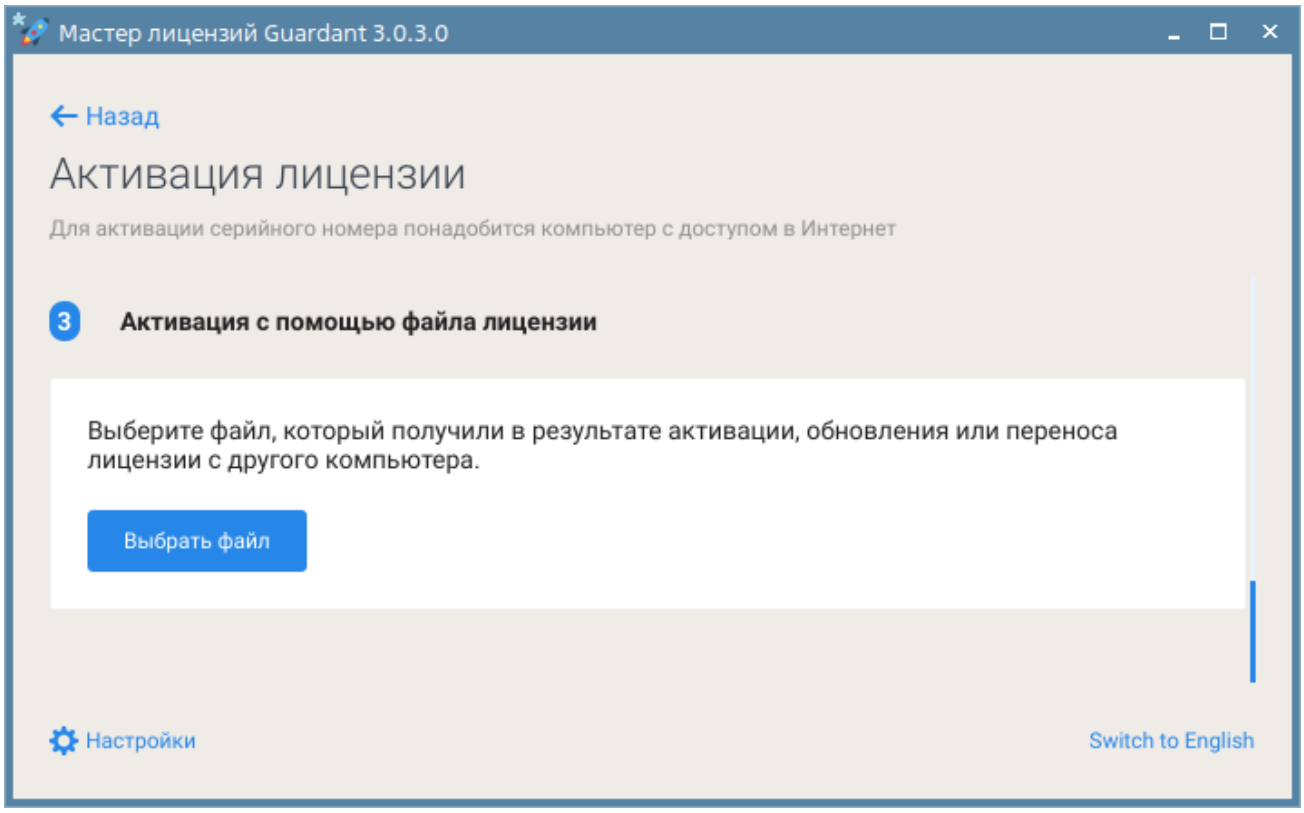


5.7. Перенесите полученный файл активации лицензии формата `*.license` на компьютер без доступа в Интернет, на котором требуется активировать лицензию.

6. На компьютере без доступа в Интернет нажмите кнопку **Продолжить, у меня есть файл лицензии**.

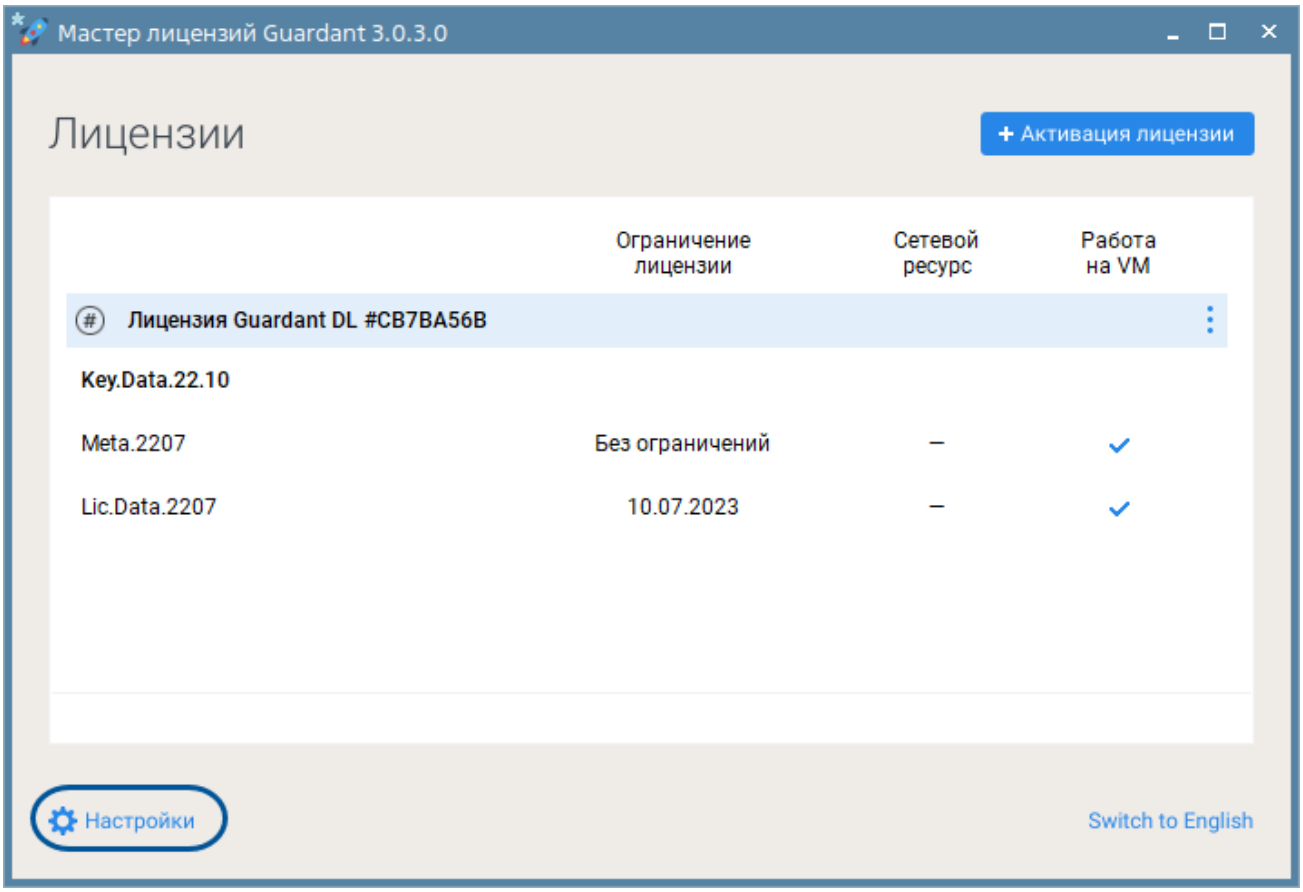


7. Нажмите кнопку **Выбрать файл** и выберите файл формата `*.license`, перенесенный с компьютера с доступом в Интернет.



Обновление на компьютере с доступом в Интернет

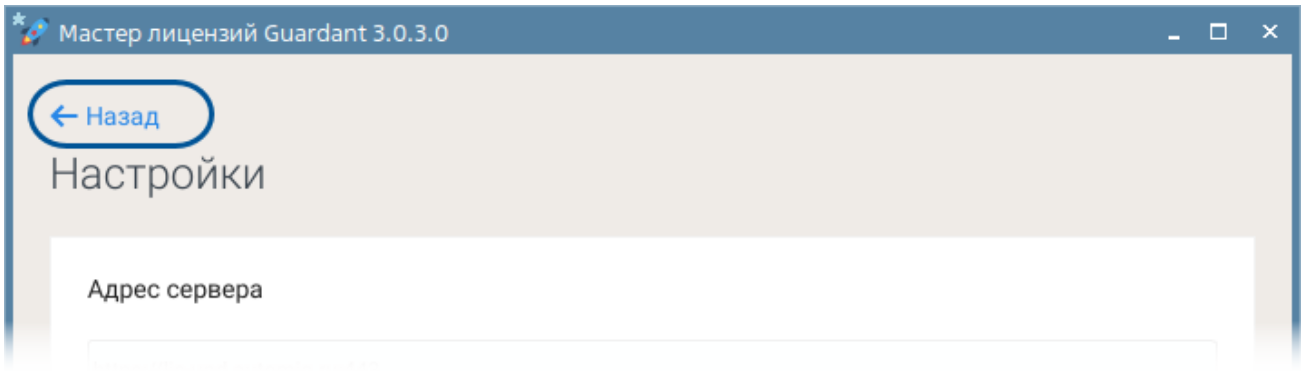
1. Запустите Мастер лицензий Guardant.
2. Перейдите в **Настройки**:



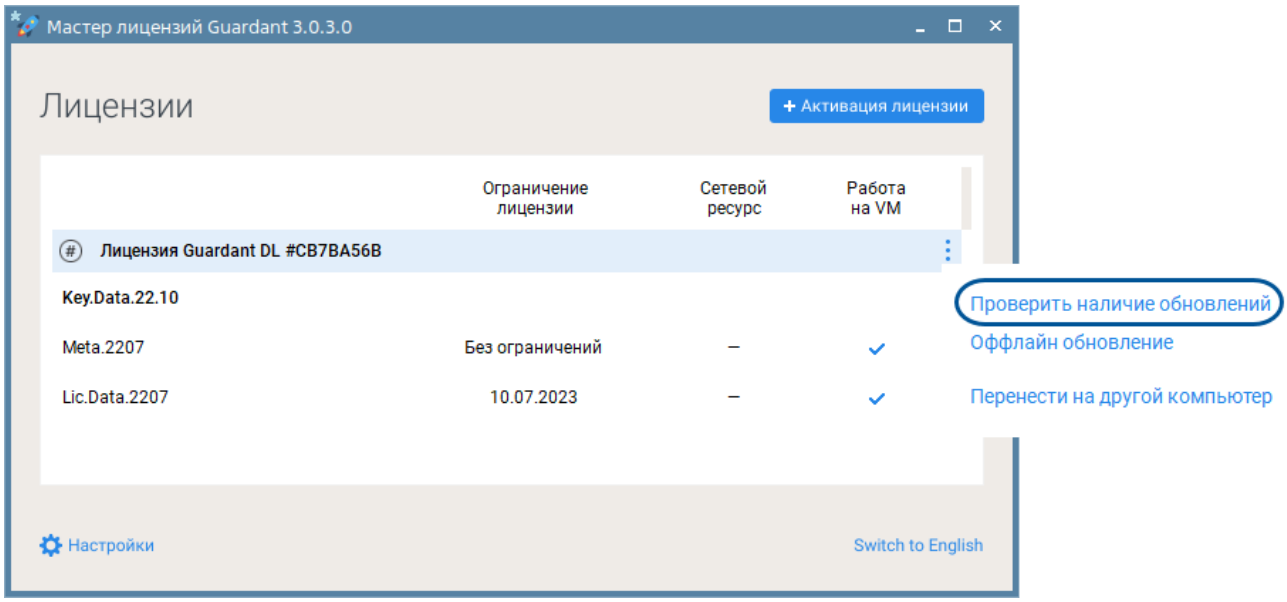
3. Укажите адрес сервера обновления лицензий:

```
https://licsep.systeme.ru:443
```

4. Вернитесь в окно **Лицензии**, нажав **Назад**.



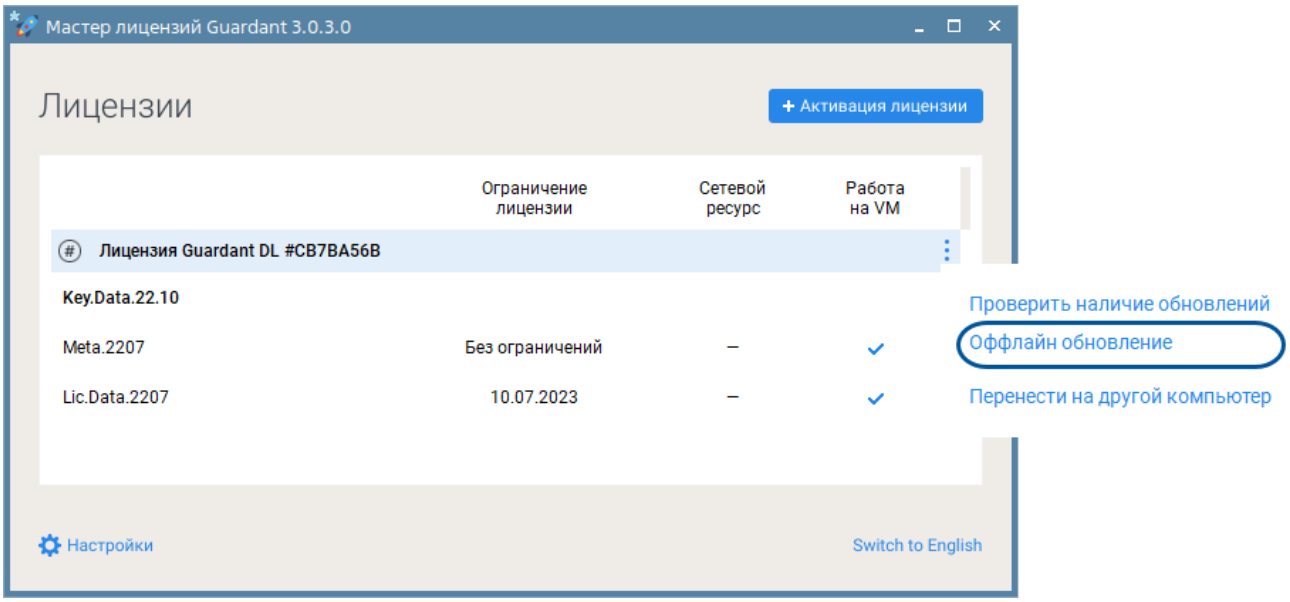
5. В окне **Лицензии** в меню ключа выберите команду **Проверить наличие обновлений**.



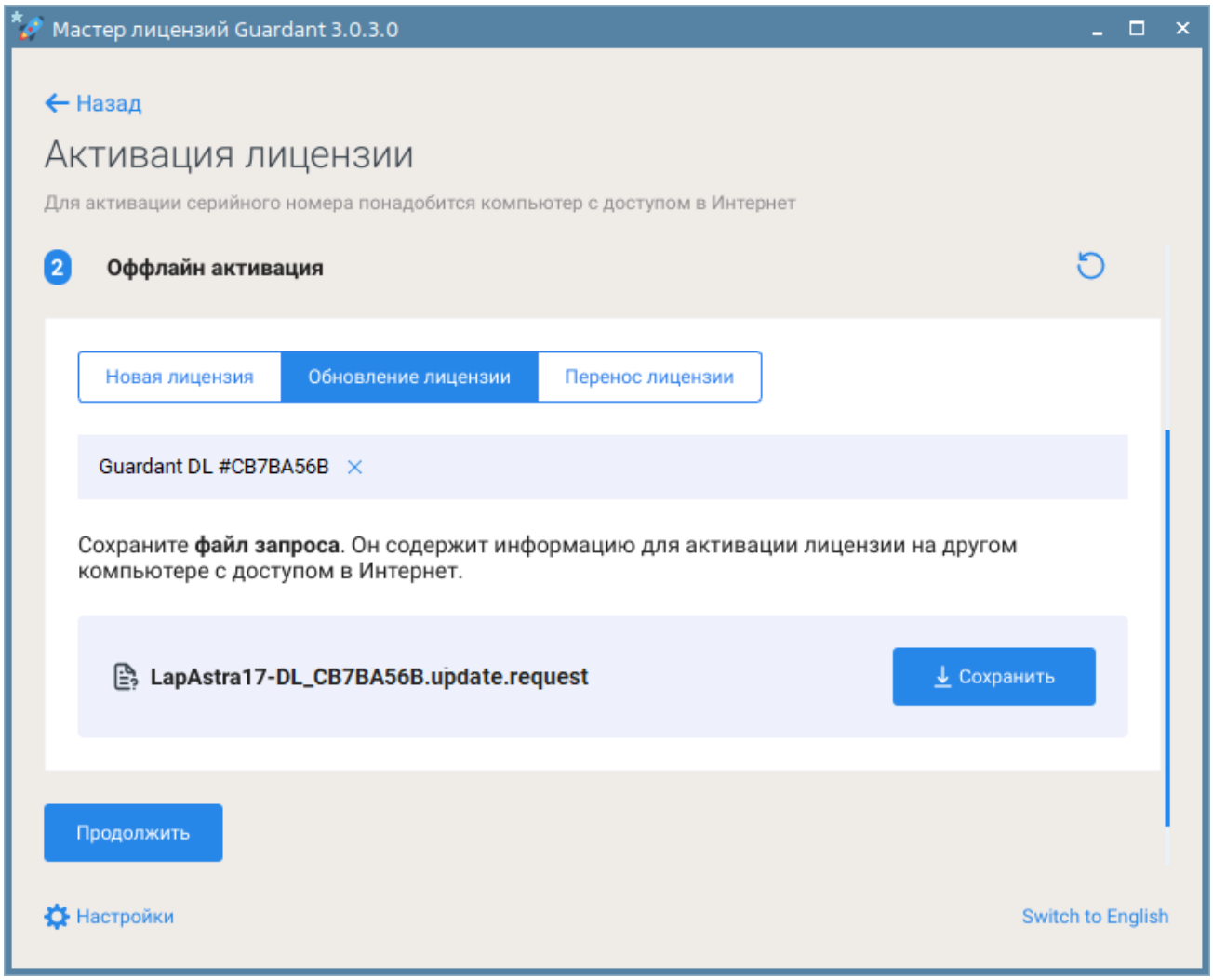
6. Если для ключа будут обнаружены обновления, то они отобразятся в списке **Обновления лицензий**. Для обновления лицензии ключа нажмите кнопку **Применить**.

Обновление на компьютере без доступа в Интернет

1. Запустите приложение Мастер лицензий Guardant.
2. В окне **Лицензии** в меню ключа выберите команду **Оффлайн обновление**.



3. На вкладке **Обновление лицензии** нажмите кнопку **Сохранить**, сохраните на диске файл запроса формата `*.request` и нажмите кнопку **Продолжить**.

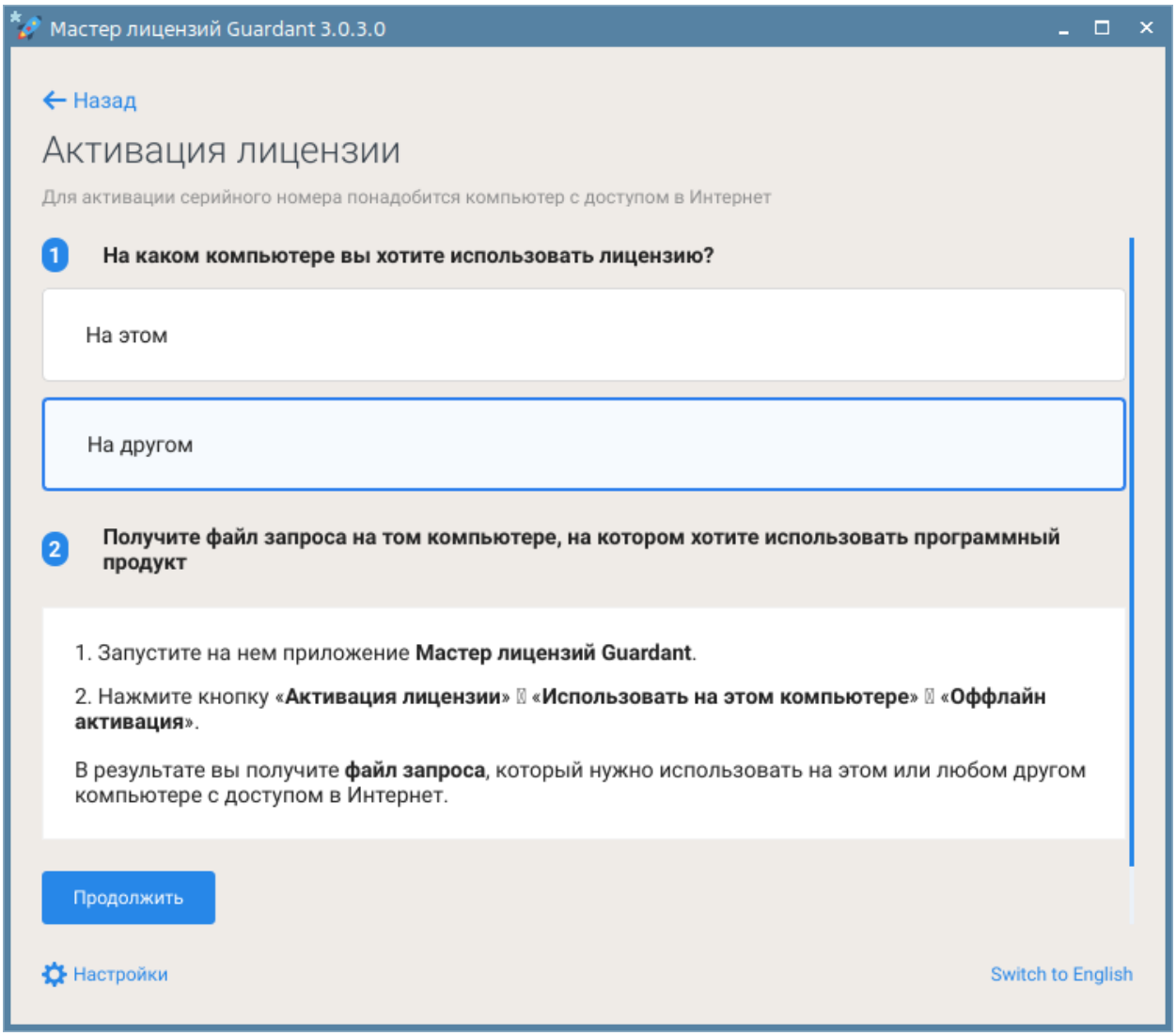


4. Перейдите на компьютер с доступом в Интернет и запустите приложение Мастер лицензий Guardant.
   4.1. Перейдите в **Настройки** и укажите адрес сервера обновления лицензий.

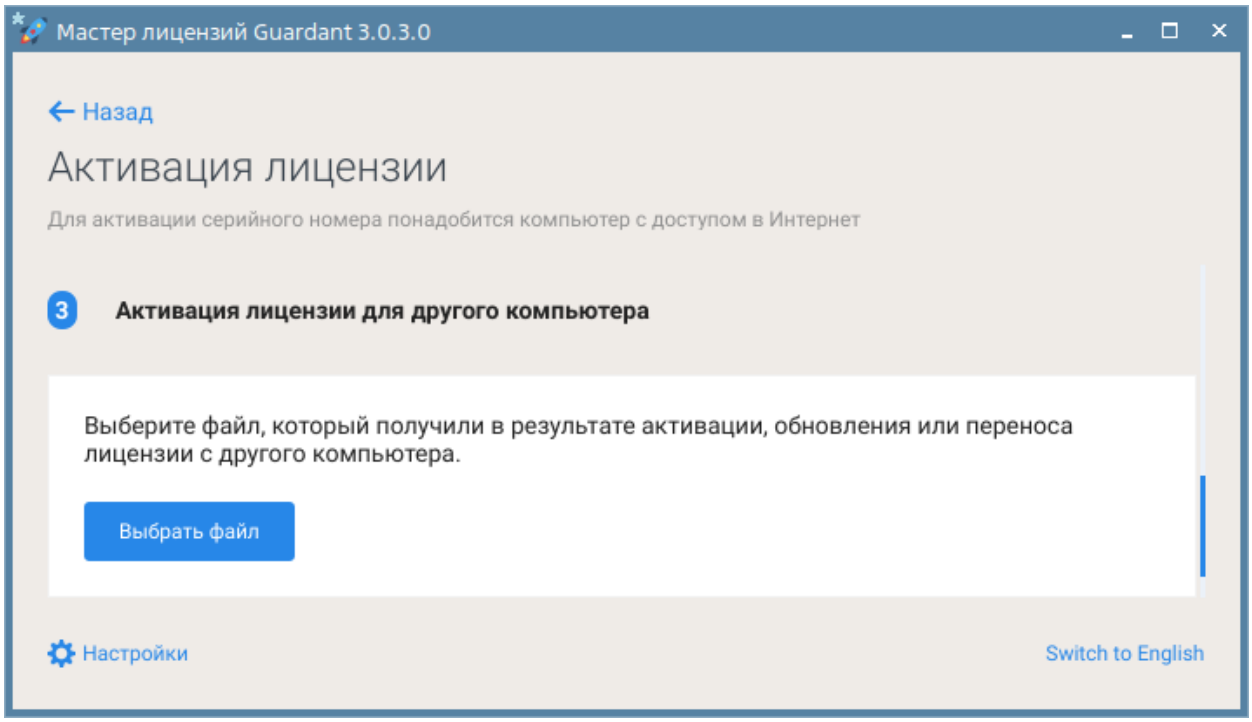
```
https://licsep.systeme.ru:443
```

   4.2. Вернитесь в окно **Лицензии** и нажмите кнопку **Активация лицензии**.

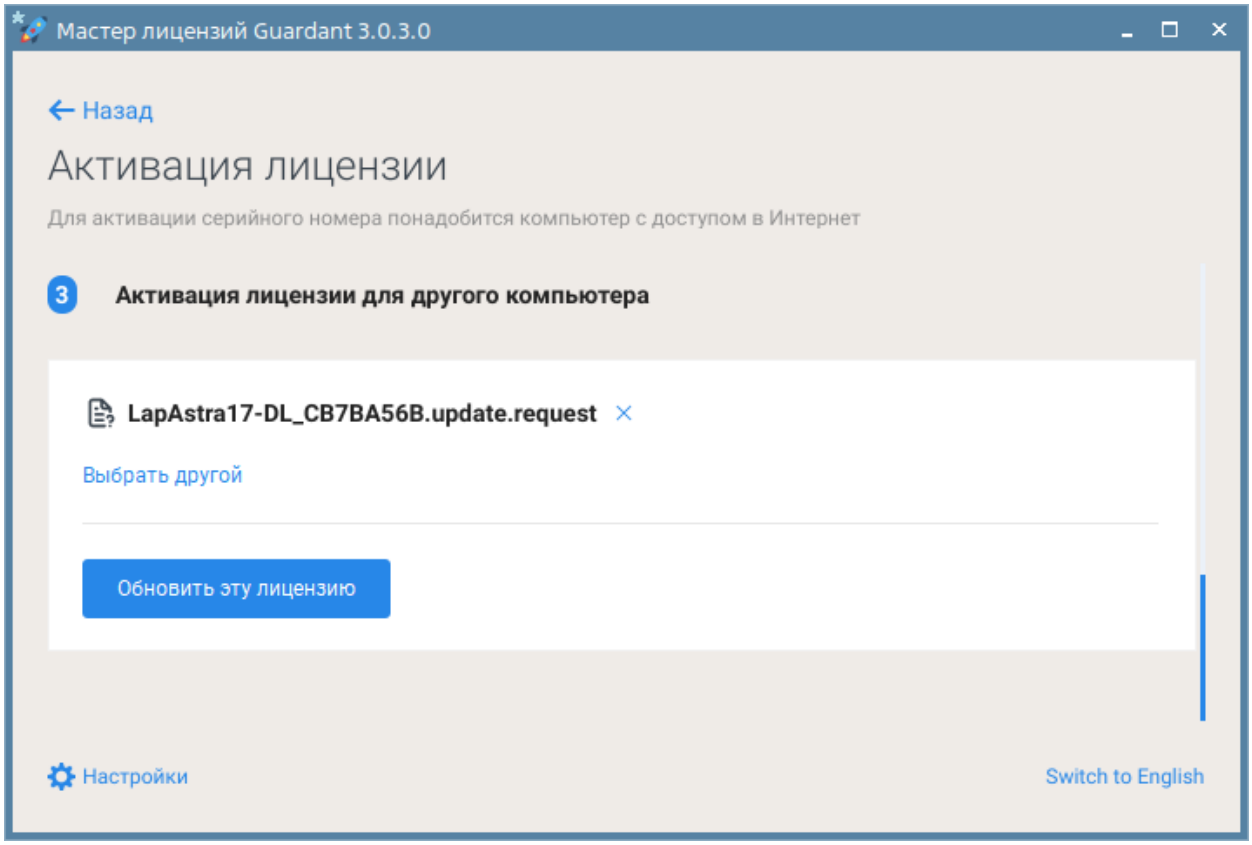
4.3. Укажите компьютер, на котором будет использоваться лицензия - **На другом** и нажмите кнопку **Продолжить**.



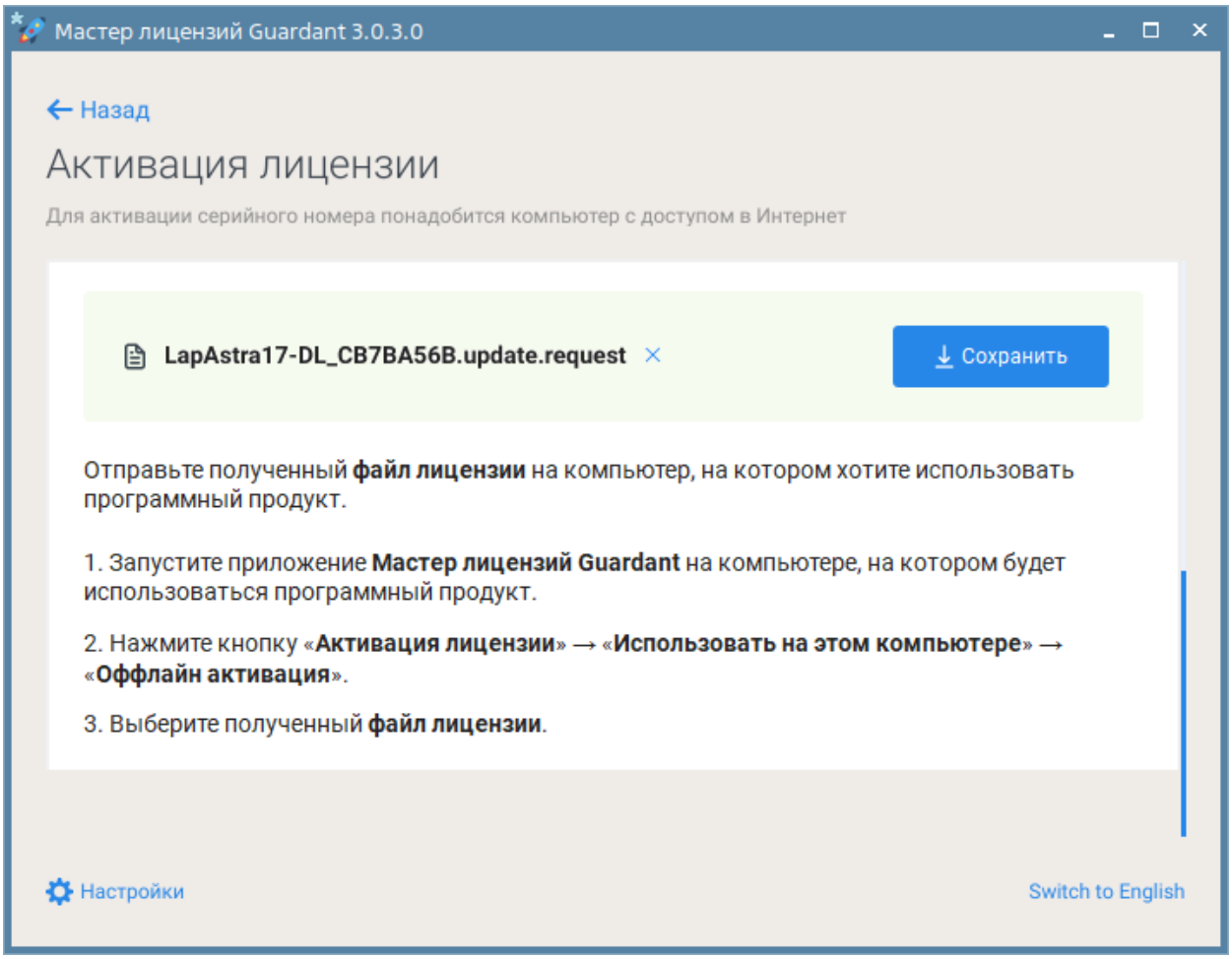
4.4. Нажмите кнопку **Выбрать файл** и выберите файл запроса формата `*.request`, перенесенный с компьютера без доступа в Интернет.



4.5. Нажмите кнопку **Обновить эту лицензию**.

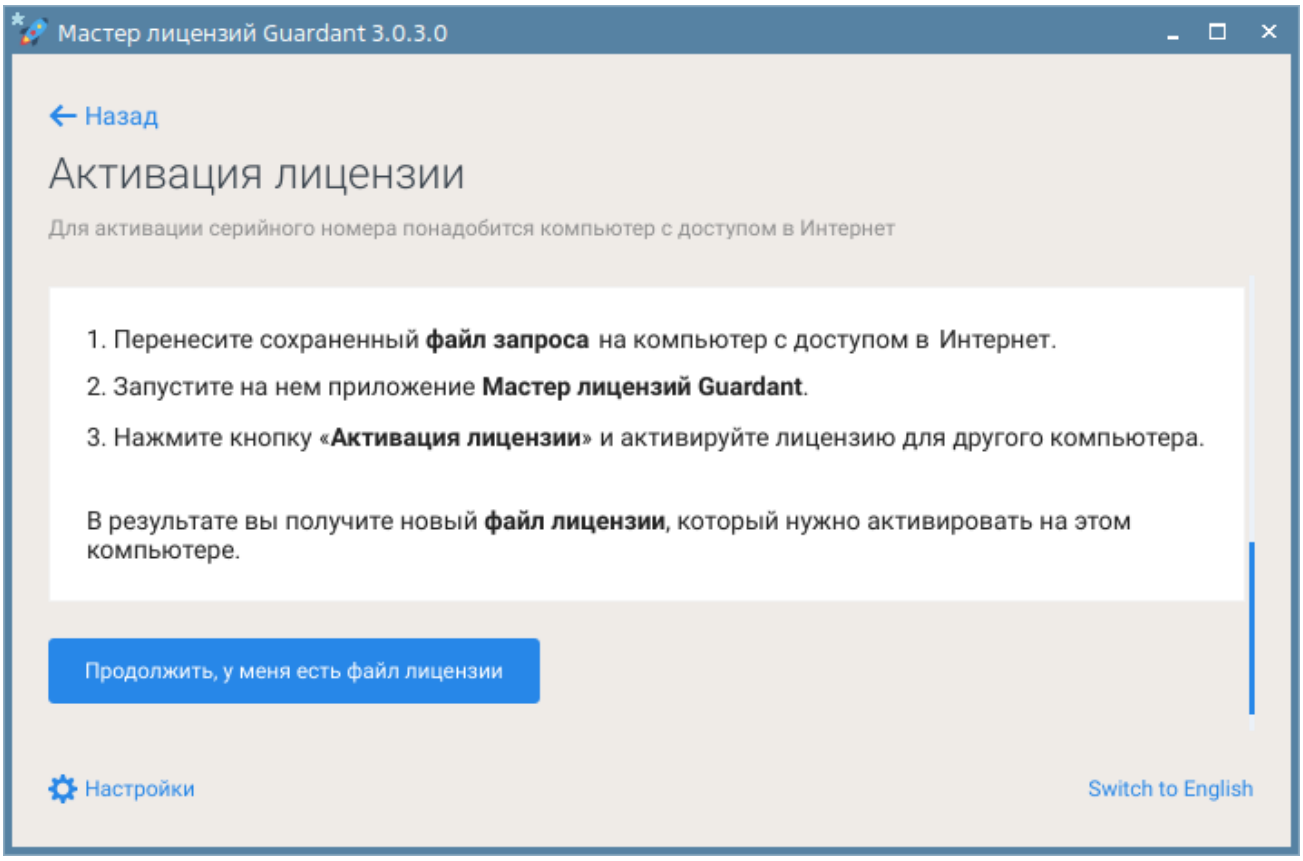


4.6. Нажмите кнопку **Сохранить** и сохраните на диске файл обновления лицензии формата `*.license`.

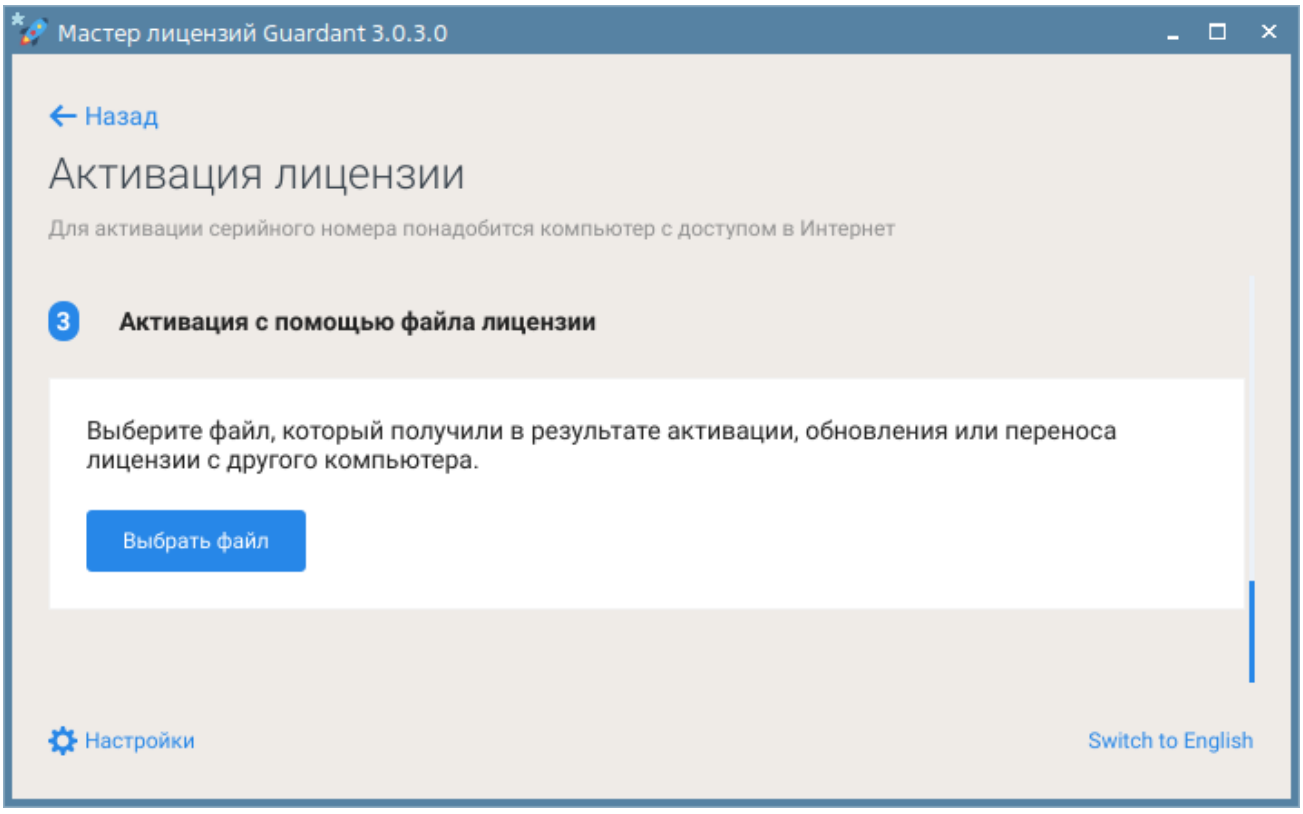


4.7. Перенесите полученный файл обновления лицензии формата `*.license` на компьютер без доступа в Интернет, на котором требуется активировать лицензию.

5. На компьютере без доступа в Интернет нажмите кнопку **Продолжить, у меня есть файл лицензии**.

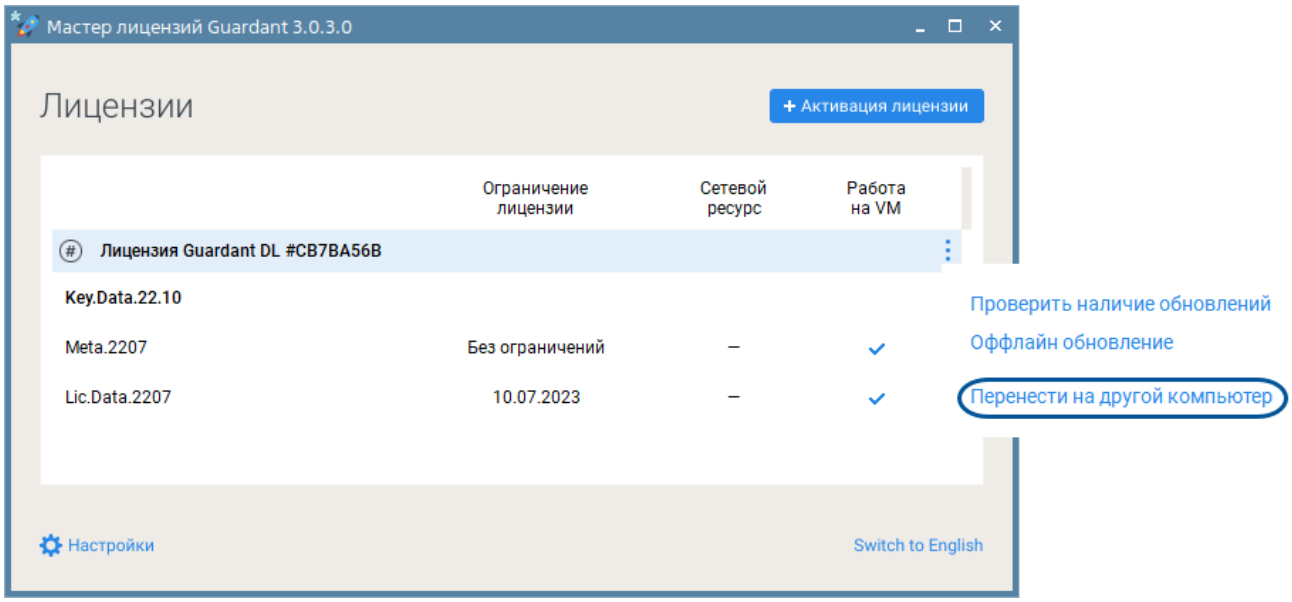


6. Нажмите кнопку **Выбрать файл** и выберите файл формата `*.license`, перенесенный с компьютера с доступом в Интернет.

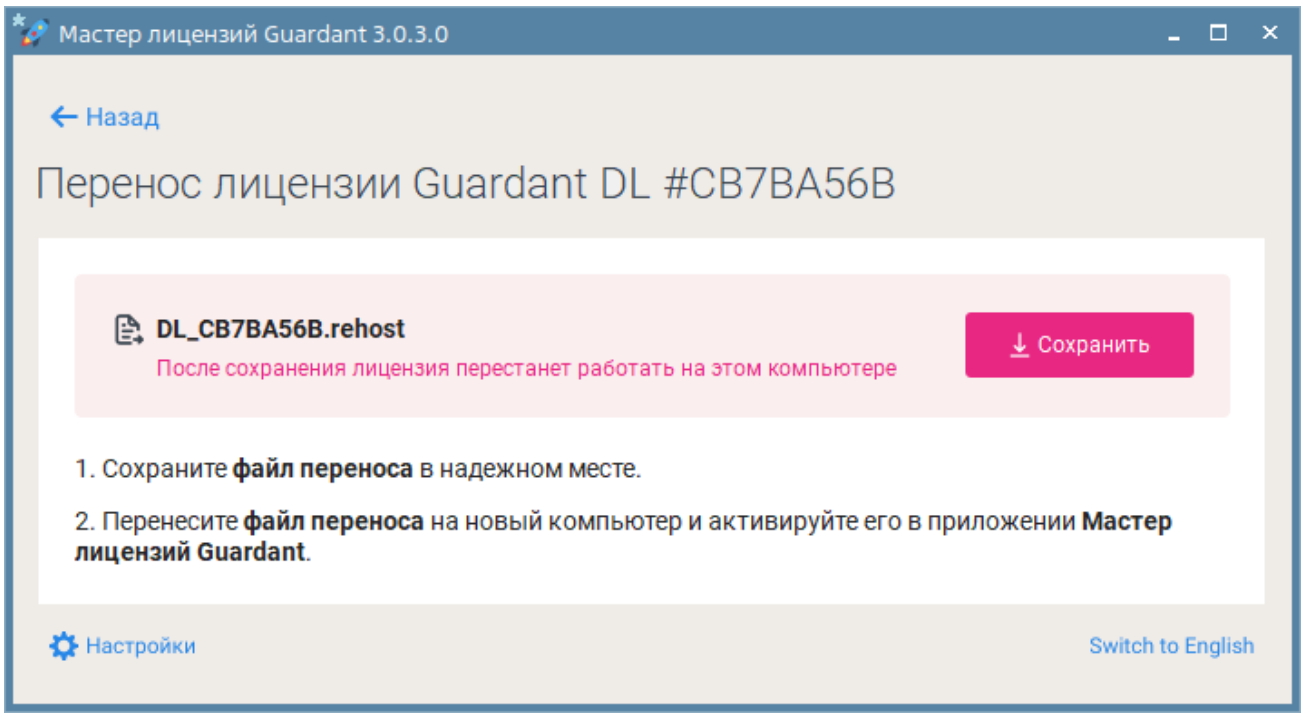


Перенос на другой компьютер

1. Запустите приложение Мастер лицензий Guardant.
2. В окне **Лицензии** в меню ключа выберите команду **Перенести на другой компьютер**.

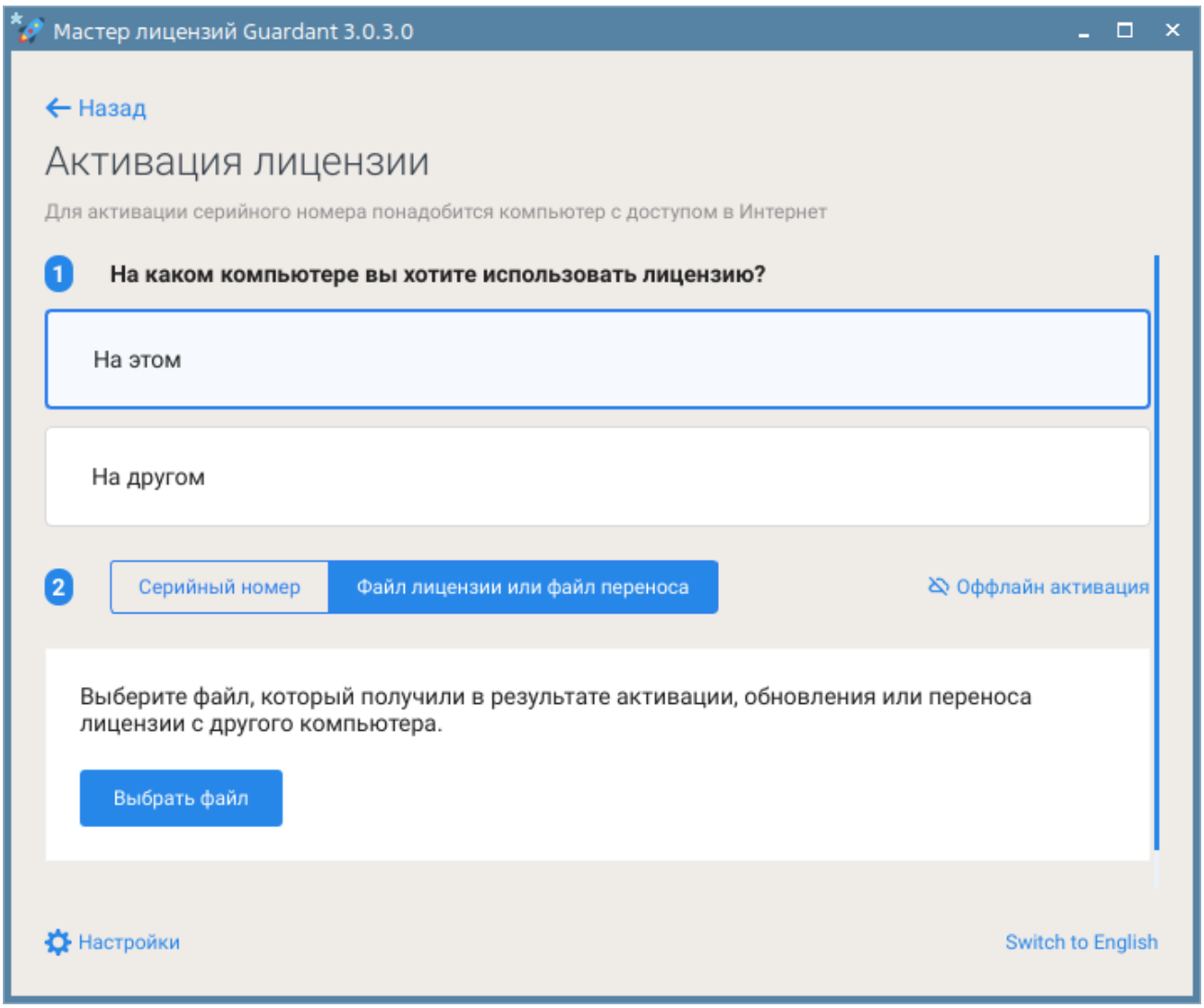


3. В окне **Перенос лицензии Guardant DL** нажмите кнопку **Сохранить** и сохраните на диске файл переноса формата `*.rehost`.



4. На другом компьютере запустите приложение Мастер лицензий Guardant и нажмите кнопку **Активация лицензии**.

5. Укажите компьютер, на котором будет использоваться лицензия - **На этом**, перейдите на вкладку **Файл лицензии или файл переноса**, нажмите кнопку **Выбрать файл** и выберите ранее сохраненный файл переноса формата `*.rehost`.



16.2. Ключи Sentinel

Для лицензирования компонентов Систэм Платформ используются два типа ключей: аппаратный ключ Sentinel HL и программный ключ Sentinel SL.

16.2.1. ОС Windows

Для лицензирования компонентов Систэм Платформ установите сервер лицензирования SePlatform.License Server.

16.2.1.1. Установка SePlatform.License Server

Для установки SePlatform.License Server запустите установочный файл `SePlatform.LicenseServer.Agent-x.x.x+xx.xxxxx-x64.msi` и следуйте инструкциям мастера установки.

Установка выполняется в папку: `C:\Program Files\SePlatform\SePlatform.LicenseServer.Agent`.

В ОС Windows SePlatform.License Server функционирует в виде службы **`SePlatform.LicenseServer.Agent`**.

16.2.1.2. Аппаратный ключ Sentinel HL

Подключите аппаратный ключ Sentinel HL в USB разъем компьютера. Дополнительных действий не требуется. Ключ готов к работе.

Обновление лицензии

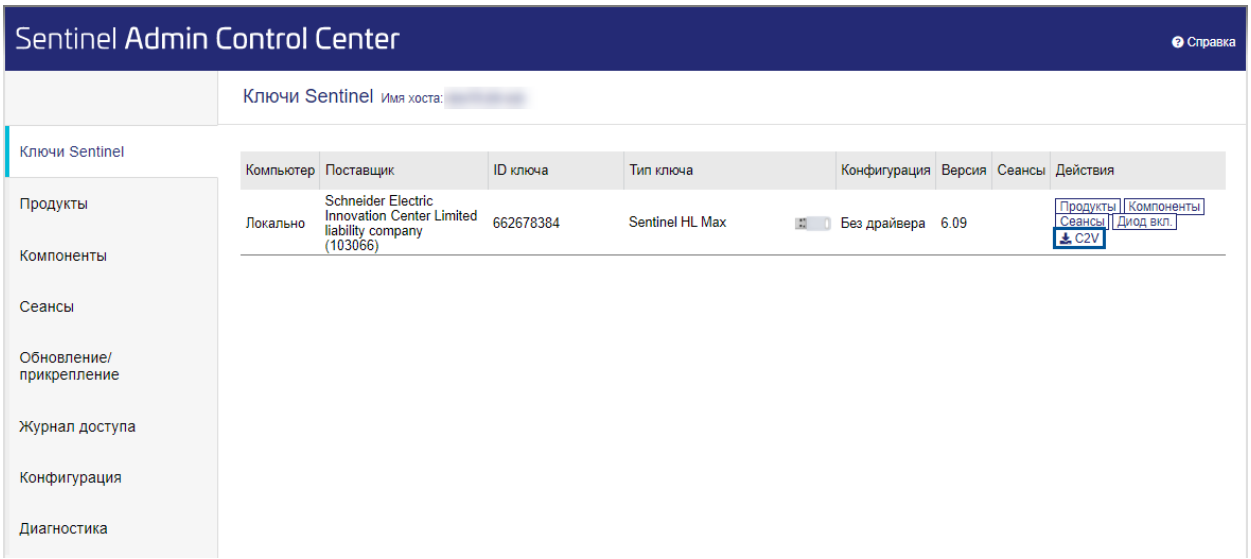
Обновление набора лицензий аппаратного ключа выполняется через web-интерфейс **`Sentinel Admin Control Center`**, который доступен по адресу http://127.0.0.1:1947/ после установки драйвера Sentinel HASP.

ПРИМЕЧАНИЕ

Если драйвер Sentinel HASP не был установлен ранее, установите его, запустив установочный файл `HASPUserSetup.exe` (расположен в папке `\Сторонние компоненты\HASPDriver`). Также загрузить архив с драйвером для Windows `Sentinel_LDK_Run-time_setup.zip` можно со страниц:

- https://cpl.thalesgroup.com/software-monetization/sentinel-drivers
- https://www.euromobile.ru/download-center/

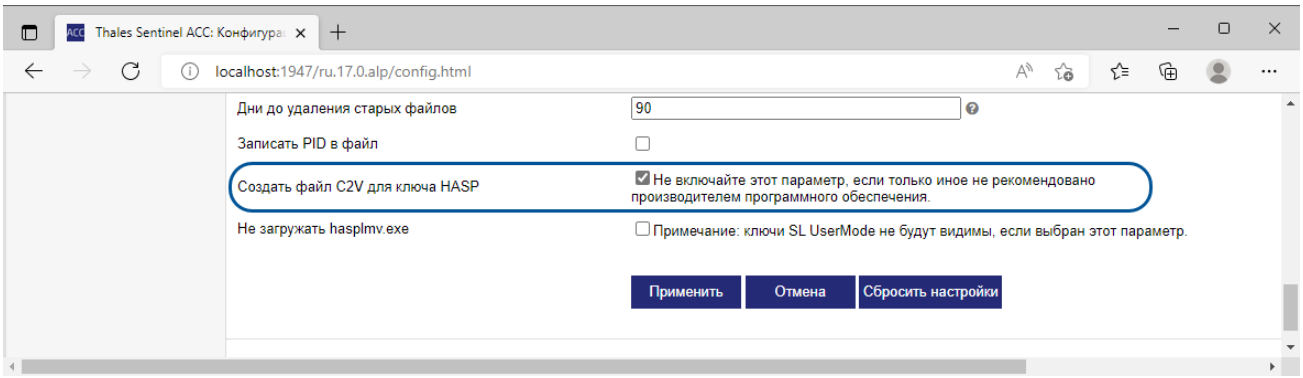
1. На компьютере с подключенным ключом в web-браузере откройте страницу http://127.0.0.1:1947/.
   1.1. В разделе **`Ключи Sentinel`** для нужного ключа нажмите кнопку **`C2V`**.



1.2. Сохраните файл образа ключа формата `*.c2v` на диске.

> ПРИМЕЧАНИЕ
>
> `*.c2v` - **«Customer To Vendor»** - файл образа ключа

Если кнопка **C2V** отсутствует в web-интерфейсе, то в разделе **Конфигурация** установите флаг **Создать файл C2V для ключа HASP** и нажмите кнопку **Применить**:

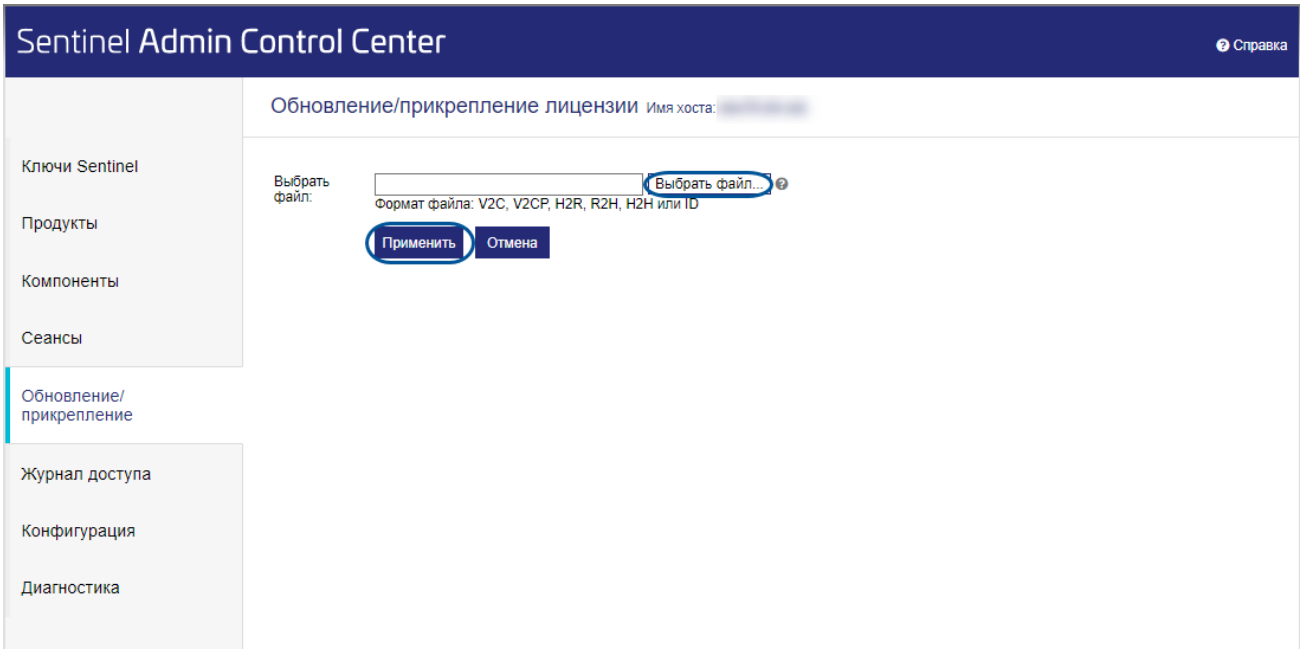


> ПРИМЕЧАНИЕ
>
> В ОС Windows при отсутствии в web-интерфейсе кнопки **C2V** для обновления набора лицензий аппаратного ключа можно воспользоваться утилитой `SePlatform Soft Rus.exe`.

2. Сгенерированный файл образа ключа формата `*.c2v` отправьте на электронную почту `support@systemesoft.ru`. В ответном письме будет выслан файл обновления набора лицензий формата `*.v2c`.

> ПРИМЕЧАНИЕ
>
> `*.v2c` - **«Vendor To Customer»** - файл набора лицензий

3. Перейдите в раздел **Обновление/прикрепление**. Нажмите кнопку **Выбрать файл...**, выберите полученный файл обновления набора лицензий формата `*.v2c` и нажмите кнопку **Применить**.



4. Перезапустите службу сервера лицензирования **`SePlatform.LicenseServer.Agent`**, после чего набор лицензий аппаратного ключа Sentinel HL будет обновлен.

16.2.1.3. Программный ключ Sentinel SL

Для работы программного ключа Sentinel SL необходимо установить драйвер Sentinel HASP.

Активация и обновление набора лицензий программного ключа Sentinel SL выполняется через web-интерфейс **`Sentinel Admin Control Center`**, который доступен по адресу http://127.0.0.1:1947/ после установки драйвера Sentinel HASP.

В ОС Windows для активации, обновления и переноса на другой компьютер программного ключа Sentinel SL Систэм Платформ можно использовать утилиту `SePlatform Soft Rus.exe`.

ОБРАТИТЕ ВНИМАНИЕ

Программный ключ Sentinel SL может быть активирован только на одном компьютере.

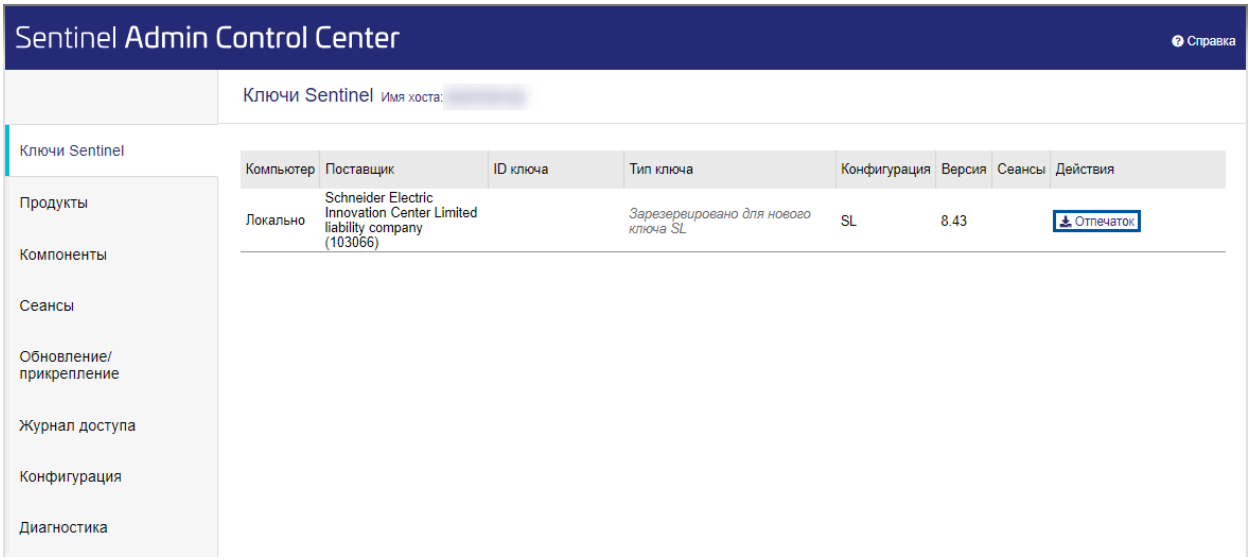
Установка драйвера Sentinel HASP

Чтобы установить драйвер Sentinel HASP, запустите установочный файл `HASPUserSetup.exe` (расположен в папке `\Сторонние компоненты\HASPDriver`). Также загрузить архив с драйвером для Windows `Sentinel_LDK_Run-time_setup.zip` можно со страниц:

- https://cpl.thalesgroup.com/software-monetization/sentinel-drivers
- https://www.euromobile.ru/download-center/

Активация

1. На компьютере в web-браузере откройте страницу http://127.0.0.1:1947/.
   1.1. В разделе **`Ключи Sentinel`** для нового ключа SL нажмите кнопку **`Отпечаток`**.



   1.2. Сохраните файл формата `*.c2v` на диске.

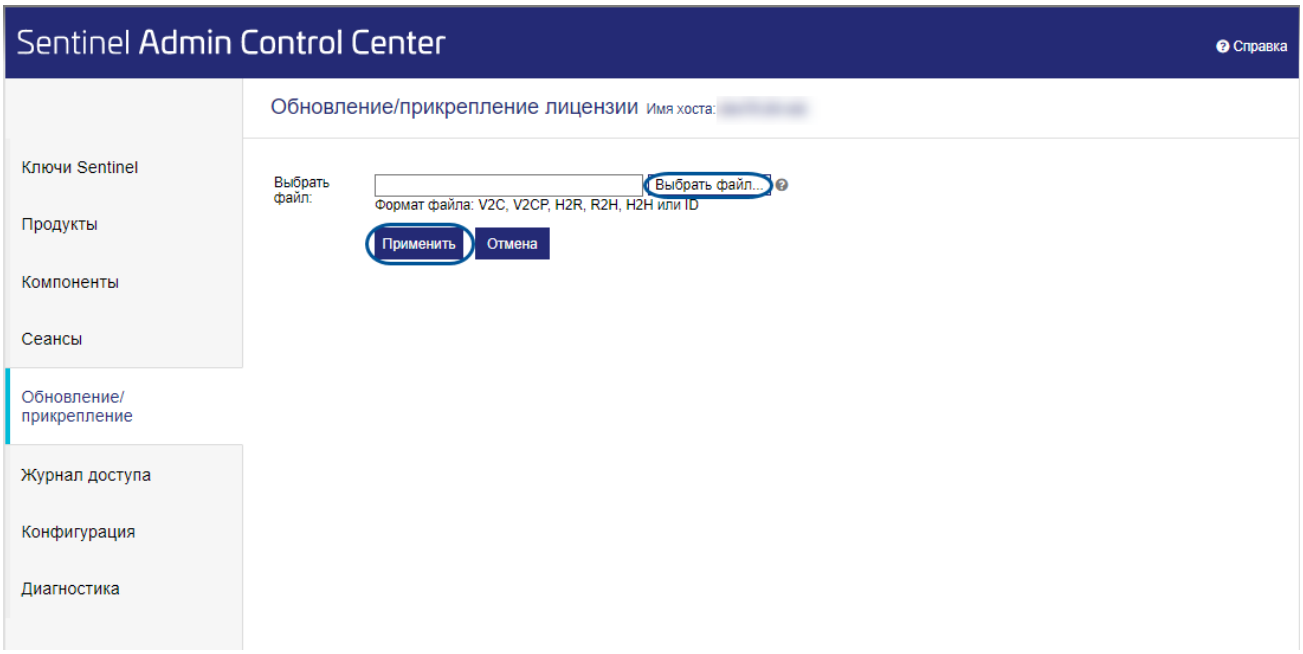
ПРИМЕЧАНИЕ

`*.c2v` - **«`Customer To Vendor`»** - файл образа системы

2. Сгенерированный файл образа системы формата `*.c2v` отправьте на электронную почту `support@systemesoft.ru`. В ответном письме будет выслан файл активации лицензии формата `*.v2c`.

> ПРИМЕЧАНИЕ
>
> `*.v2c` - **«Vendor To Customer»** - файл активации лицензии

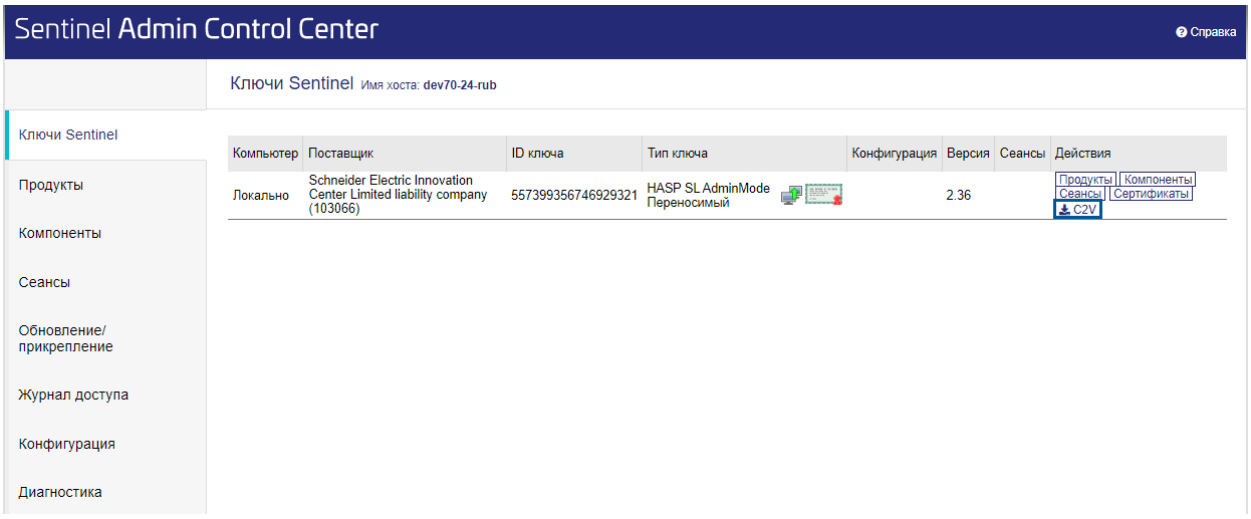
3. Перейдите в раздел **Обновление/прикрепление**. Нажмите кнопку **Выбрать файл...**, выберите полученный файл активации лицензии формата `*.v2c` и нажмите кнопку **Применить**.



4. Перезапустите службу сервера лицензирования **`SePlatform.LicenseServer.Agent`**, после чего программный ключ Sentinel SL будет активирован.

Обновление

1. На компьютере в web-браузере откройте страницу http://127.0.0.1:1947/.
   1.1. В разделе **Ключи Sentinel** для нужного ключа нажмите кнопку **C2V**.



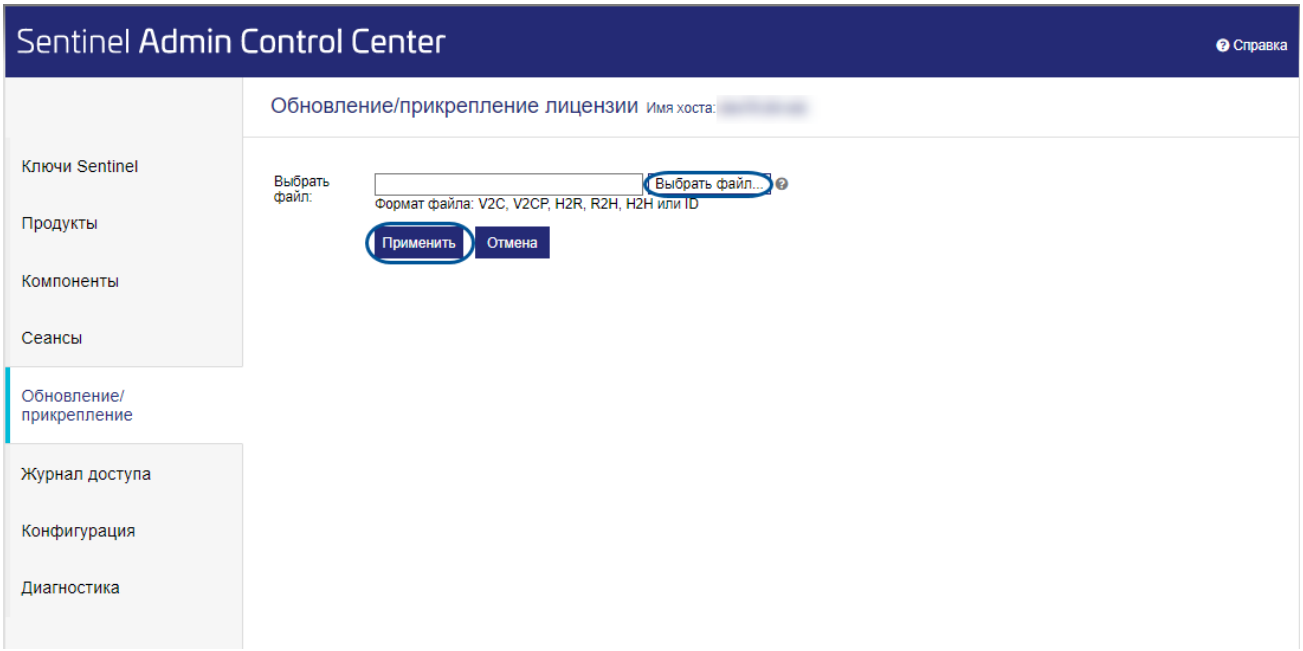
1.2. Сохраните файл образа ключа формата `*.c2v` на диске.

> ПРИМЕЧАНИЕ
>
> `*.c2v` - **«Customer To Vendor»** - файл образа ключа

2. Сгенерированный файл образа ключа формата `*.c2v` отправьте на электронную почту `support@systemesoft.ru`. В ответном письме будет выслан файл обновления набора лицензий формата `*.v2c`.

> ПРИМЕЧАНИЕ
>
> `*.v2c` - **«Vendor To Customer»** - файл набора лицензий

3. Перейдите в раздел **Обновление/прикрепление**. Нажмите кнопку **Выбрать файл...**, выберите полученный файл обновления набора лицензий формата `*.v2c` и нажмите кнопку **Применить**.



4. Перезапустите службу сервера лицензирования **SePlatform.LicenseServer.Agent**, после чего набор лицензий аппаратного ключа Sentinel HL будет обновлен.

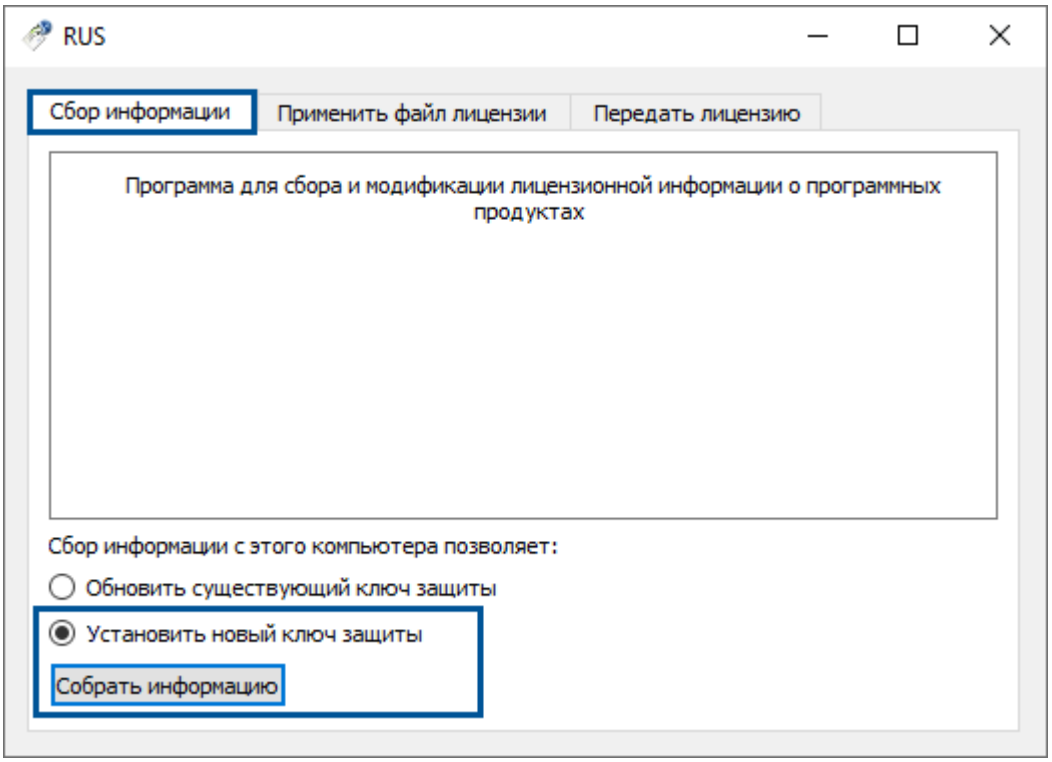
Утилита SePlatform Soft Rus.exe

В ОС Windows для активации, обновления и переноса на другой компьютер программного ключа Sentinel SL Систэм Платформ может использоваться утилита `SePlatform Soft Rus.exe` (расположена в папке `\Сторонние компоненты\HASPDriver\SePlatform Soft Rus`).

> ПРИМЕЧАНИЕ
>
> Если в процессе работы с утилитой появилось сообщение **«Ошибка обновления: Библиотека производителя не найдена»**, то из папки утилиты скопируйте файл `haspvlib_xxxxxx.dll` в папку `C:\Program Files (x86)\Common Files\Aladdin Shared\HASP`.

Активация

1. Запустите утилиту `SePlatform Soft Rus.exe`.
2. На вкладке **Сбор информации** выберите переключатель **Установить новый ключ защиты** и нажмите кнопку **Собрать информацию**.



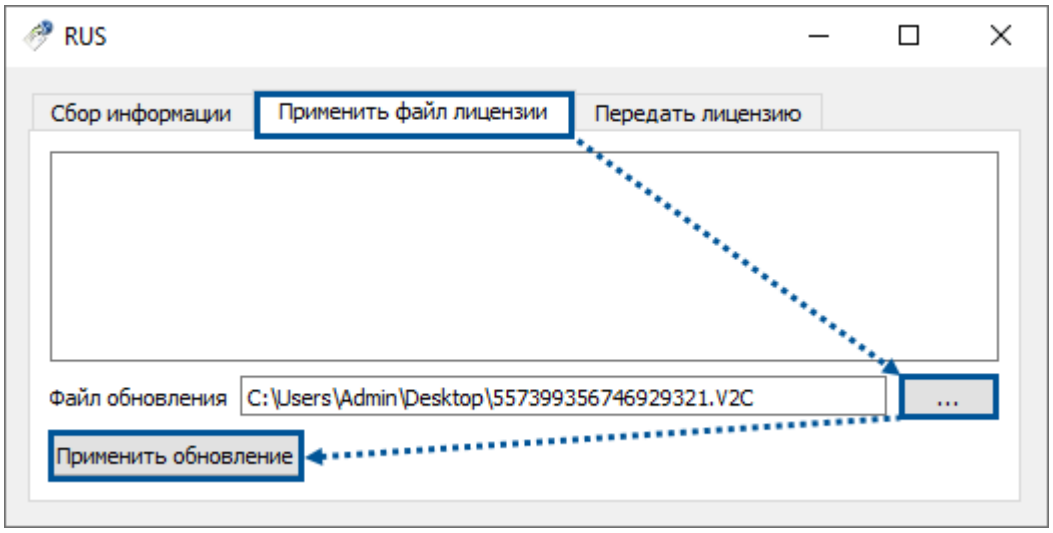
3. В открывшемся окне укажите место сохранения, имя файла и нажмите кнопку **Сохранить**. Файл формата `*.c2v` будет сохранен на диск.

> ПРИМЕЧАНИЕ
>
> `*.c2v` - **«Customer To Vendor»** - файл образа ключа

4. Отправьте на электронную почту `support@systemesoft.ru` письмо, содержащее:
   - ключ продукта, указанный в сертификате из комплекта поставки;
   - сохраненный файл формата `*.c2v`.
5. В ответном письме будет выслан файл формата `*.v2c`.

> ПРИМЕЧАНИЕ
>
> `*.v2c` - **«Vendor To Customer»** - файл набора лицензий

6. На вкладке **Применить файл лицензии** утилиты `SePlatform Soft Rus.exe` нажмите кнопку ..., выберите полученный файл формата `*.v2c` и нажмите кнопку **Применить обновление**.

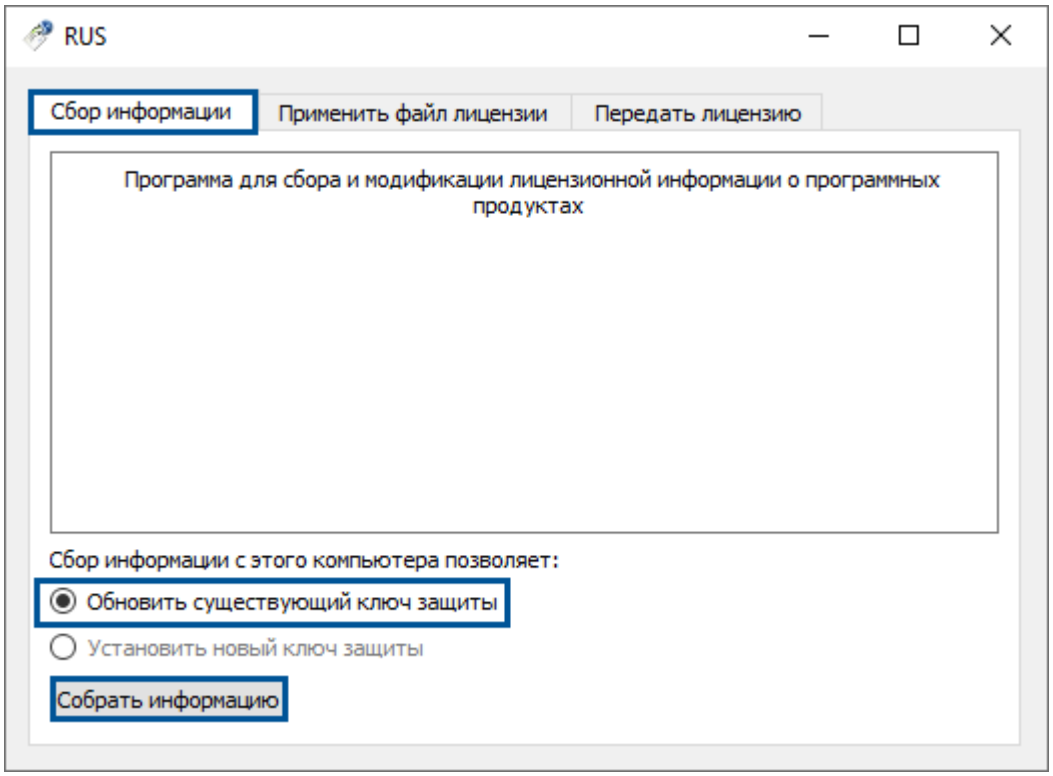


Программный ключ Sentinel SL активирован.

7. Перезапустите службу сервера лицензирования **`SePlatform.LicenseServer.Agent`**.

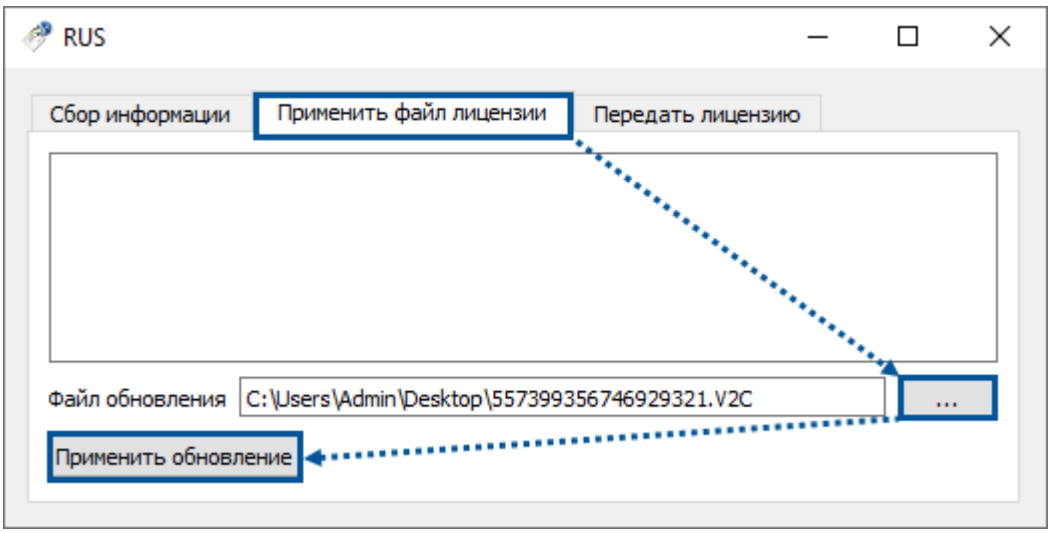
Обновление лицензии

1. Запустите утилиту `SePlatform Soft Rus.exe`.
2. На вкладке **Сбор информации** выберите переключатель **Обновить существующий ключ защиты** и нажмите кнопку **Собрать информацию**.



3. В открывшемся окне укажите место сохранения, имя файла образа ключа и нажмите кнопку **Сохранить**. Файл формата `*.c2v` будет сохранен на диск.

4. Отправьте на электронную почту `support@systemesoft.ru` письмо, содержащее:
   - ключ продукта, указанный в сертификате из комплекта поставки;
   - сохраненный файл формата `*.c2v`.
5. В ответном письме будет выслан файл обновления набора лицензий формата `*.v2c`.
6. На вкладке **Применить файл лицензии** утилиты `SePlatform Soft Rus.exe` нажмите кнопку ..., выберите полученный файл обновления набора лицензий формата `*.v2c` и нажмите кнопку **Применить обновление**.



Набор лицензий программного ключа Sentinel SL обновлён.

7. Перезапустите службу сервера лицензирования SePlatform.LicenseServer.Agent.

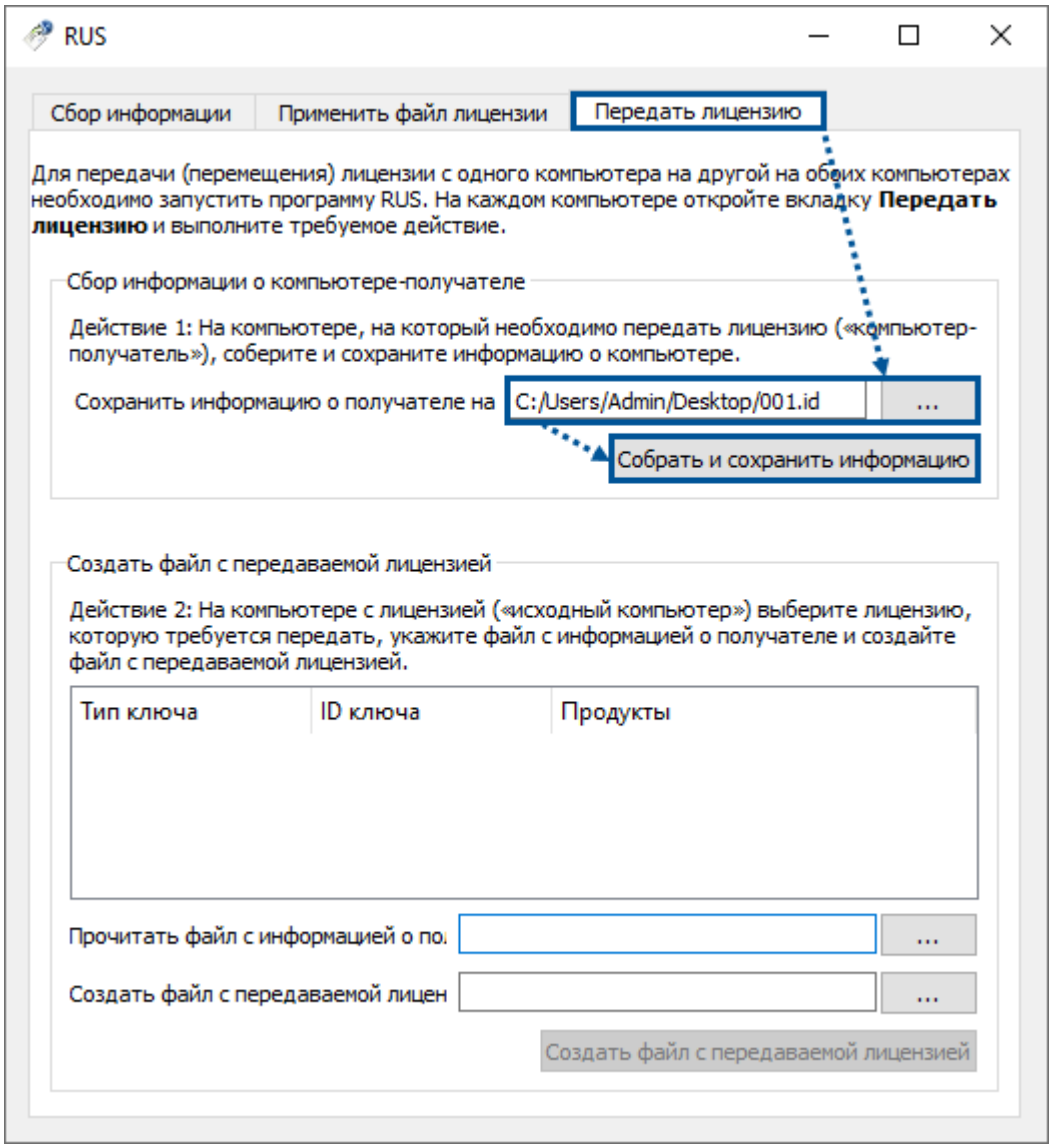
Перенос программного ключа на другой компьютер

ОБРАТИТЕ ВНИМАНИЕ

На компьютере, на который требуется перенести программный ключ, должен быть установлен драйвер Sentinel HASP.

1. Запустите утилиту `SePlatform Soft Rus.exe` на компьютере, на который требуется перенести программный ключ.

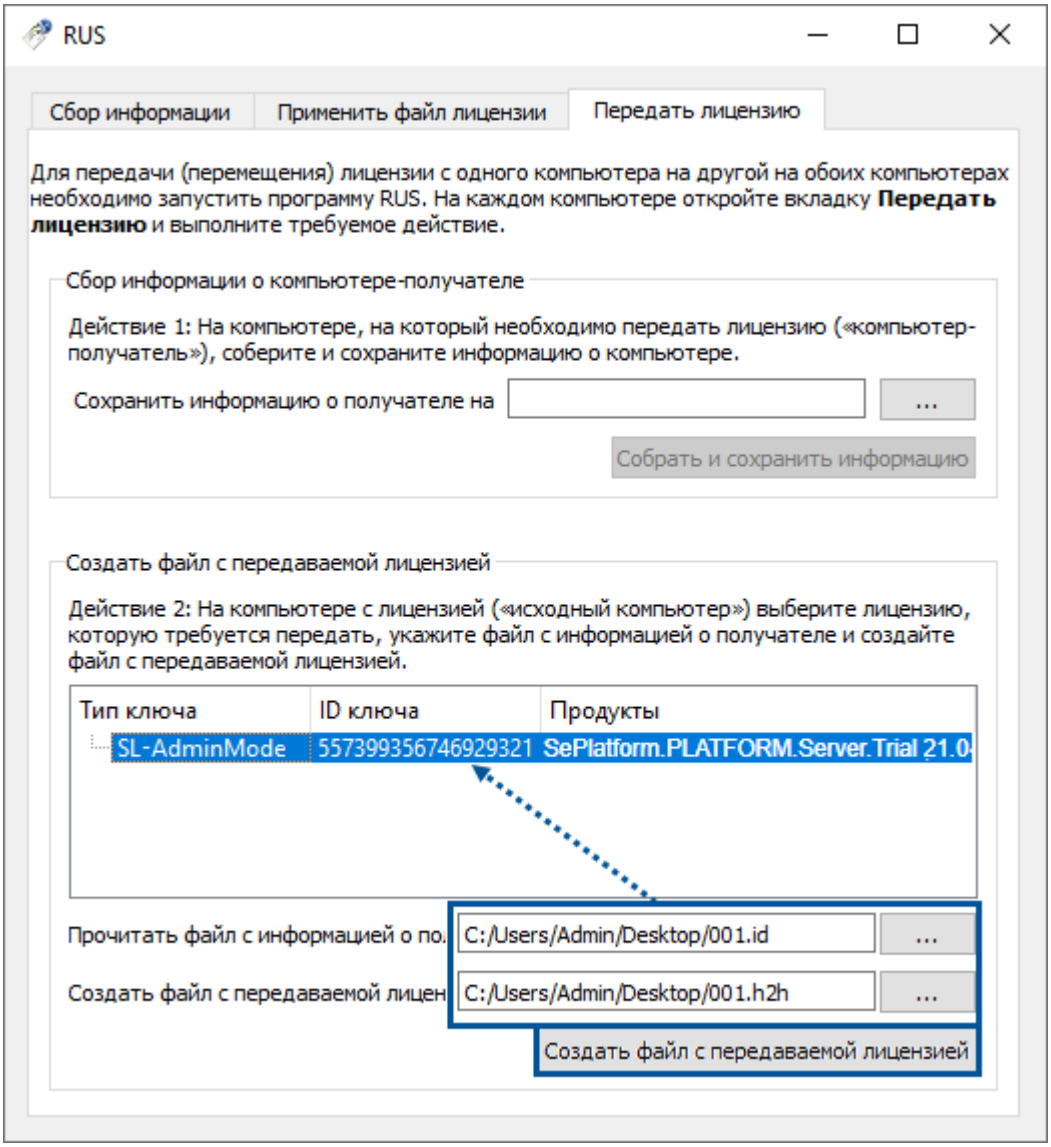
2. На вкладке **Передать лицензию** выполните генерацию ID-файла с информацией о системе. Для этого нажмите кнопку ..., укажите имя и путь для сохранения файла формата `*.id` и нажмите кнопку **Собрать и сохранить информацию**.



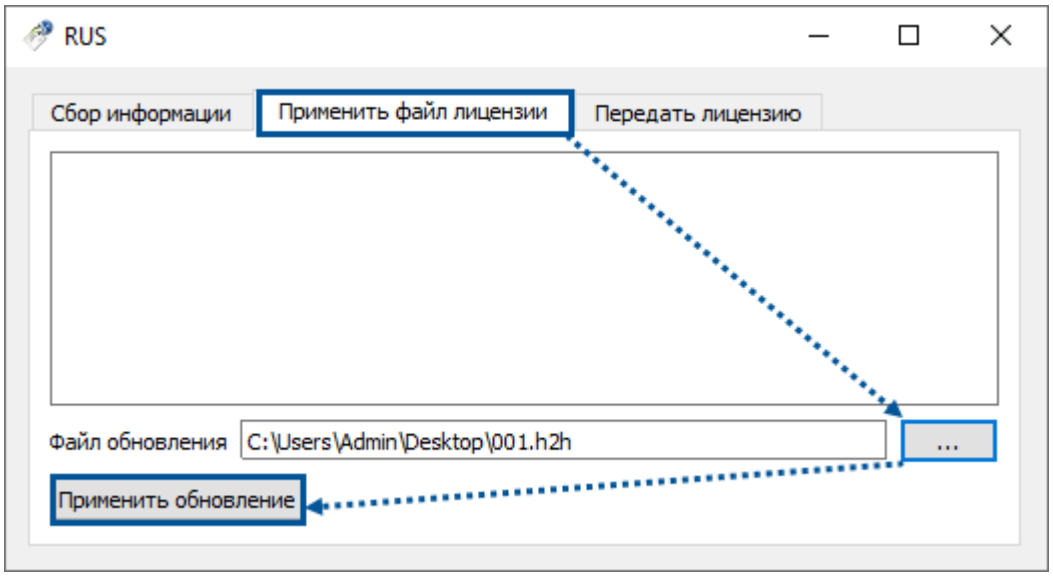
3. Запустите утилиту `SePlatform Soft Rus.exe` на компьютере, с которого требуется перенос программного ключа.

4. На вкладке **Передать лицензию**:

   - укажите путь до файла формата `*.id`, сгенерированного на компьютере, на который требуется перенести программный ключ;
   - укажите путь и имя для сохранения файла с ключом формата `*.h2h`;
   - из списка ключей выберите ключ, который требуется перенести;
   - выполните генерацию файла с переносимым ключом формата `*.h2h`, нажав кнопку **Создать файл с передаваемой лицензией**.



5. На компьютере, на который требуется перенести программный ключ, примените файл с переносимым ключом. Для этого на вкладке **Применить файл лицензии** нажмите кнопку ..., выберите сгенерированный файл формата `*.h2h` и нажмите кнопку **Применить обновление**.



Программный ключ Sentinel SL перенесен.

6. Перезапустите службу сервера лицензирования SePlatform.LicenseServer.Agent.

16.2.2. ОС Linux

Для лицензирования компонентов Систэм Платформ, установленных на компьютере с ОС Linux:

- установите сервер лицензирования SePlatform.License Server;
- установите драйвер Sentinel HASP.

16.2.2.1. Установка SePlatform.License Server

ОБРАТИТЕ ВНИМАНИЕ

Команда установки выполняется только от суперпользователя **«root»**.

Имя устанавливаемого пакета: `seplatform.licenseserver.agent-x.x.x+xx.xxxxx.deb` или `seplatform.licenseserver.agent-x.x.x+xx.xxxxx.rpm` в зависимости от используемой ОС Linux. Находясь в папке с установочным пакетом, запустите установку штатным пакетным менеджером.
Установка пакета `*.rpm` с помощью пакетного менеджера YUM:

```
yum install seplatform.licensing.agent-x.x.x+xx.xxxxx.rpm
```

Установка пакета `*.rpm` с помощью пакетного менеджера RPM:

```
rpm -i seplatform.licensing.agent-x.x.x+xx.xxxxx.rpm
```

Установка пакета `*.deb` с помощью пакетного менеджера apt:

```
apt-get install seplatform.licensing.agent-x.x.x+xx.xxxxx.deb
```

Установка пакета `*.deb` с помощью пакетного менеджера dpkg:

```
sudo dpkg -i seplatform.licensing.agent-x.x.x+xx.xxxxx.deb
```

16.2.2.2. Установка драйвера Sentinel HASP

Чтобы установить драйвер Sentinel HASP:

1. Со страницы https://cpl.thalesgroup.com/software-monetization/sentinel-drivers или https://www.euromobile.ru/download-center/ загрузите архив с драйвером для Linux `Linux Sentinel_LDK_Run-time_linux.zip`. При этом загруженный файл архива будет называться `Sentinel_LDK_Linux_Run-time_Installer_script.tar.gz`.
2. Распакуйте загруженный архив `Sentinel_LDK_Linux_Run-time_Installer_script.tar.gz`.
3. Распакуйте архив `aksusbd-x.xx.x.tar.gz`.
4. В папку с файлом `dinst` скопируйте файл библиотеки `haspvlib_x86_64_xxxxxx.so` (расположен в папке `\Сторонние компоненты\HASPDriver\linux-vlib`).
5. Находясь в папке с файлами `dinst` и `haspvlib_x86_64_xxxxxx.so`, от суперпользователя **«root»** выполните команду:

   ```
   ./dinst .
   ```

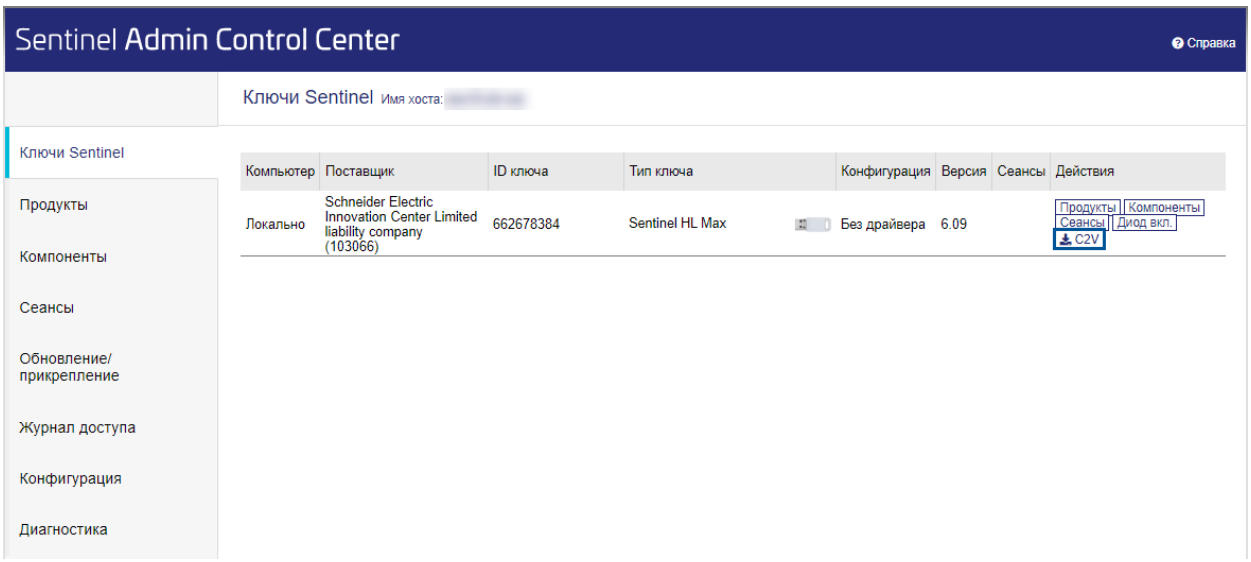
16.2.2.3. Аппаратный ключ Sentinel HL

Подключите аппаратный ключ Sentinel HL в USB разъем компьютера. Дополнительных действий не требуется. Ключ готов к работе.

Обновление лицензии

Обновление набора лицензий аппаратного ключа выполняется через web-интерфейс **`Sentinel Admin Control Center`**, который доступен по адресу http://127.0.0.1:1947/ после установки драйвера Sentinel HASP.

1. На компьютере с подключенным ключом в web-браузере откройте страницу http://127.0.0.1:1947/.
   1.1. В разделе **`Ключи Sentinel`** для нужного ключа нажмите кнопку **`C2V`**.

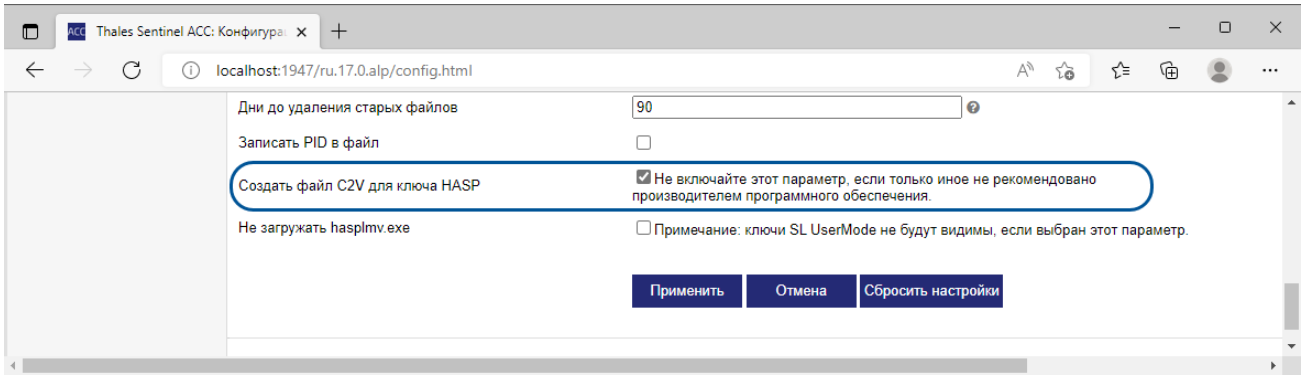


1.2. Сохраните файл образа ключа формата `*.c2v` на диске.

ПРИМЕЧАНИЕ

`*.c2v` - **«Customer To Vendor»** - файл образа ключа

Если кнопка **C2V** отсутствует в web-интерфейсе, то в разделе **Конфигурация** установите флаг **Создать файл C2V для ключа HASP** и нажмите кнопку **Применить**:

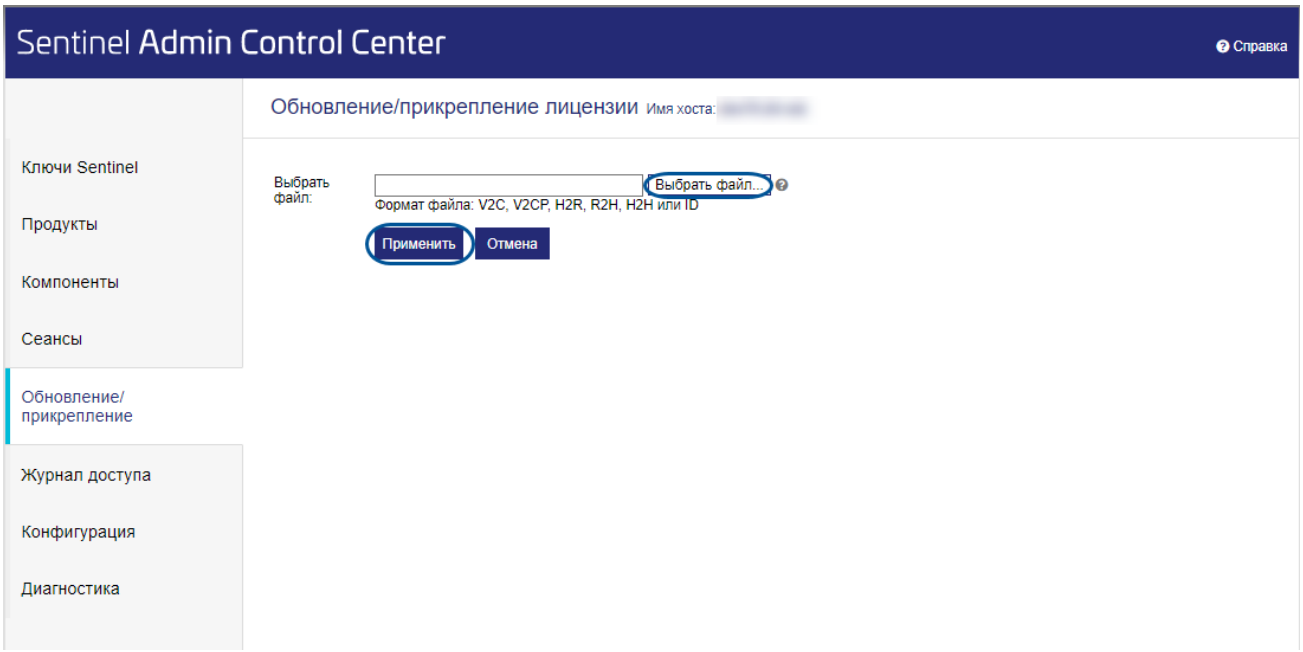


2. Сгенерированный файл образа ключа формата `*.c2v` отправьте на электронную почту `support@systemesoft.ru`. В ответном письме будет выслан файл обновления набора лицензий формата `*.v2c`.

ПРИМЕЧАНИЕ

`*.v2c` - **«Vendor To Customer»** - файл набора лицензий

3. Перейдите в раздел **Обновление/прикрепление**. Нажмите кнопку **Выбрать файл...**, выберите полученный файл обновления набора лицензий формата `*.v2c` и нажмите кнопку **Применить**.



4. Перезапустите сервис **seplatform.licenseserver.agent** командой:

```
systemctl restart seplatform.licenseserver.agent
```

После чего набор лицензий аппаратного ключа Sentinel HL будет обновлен.

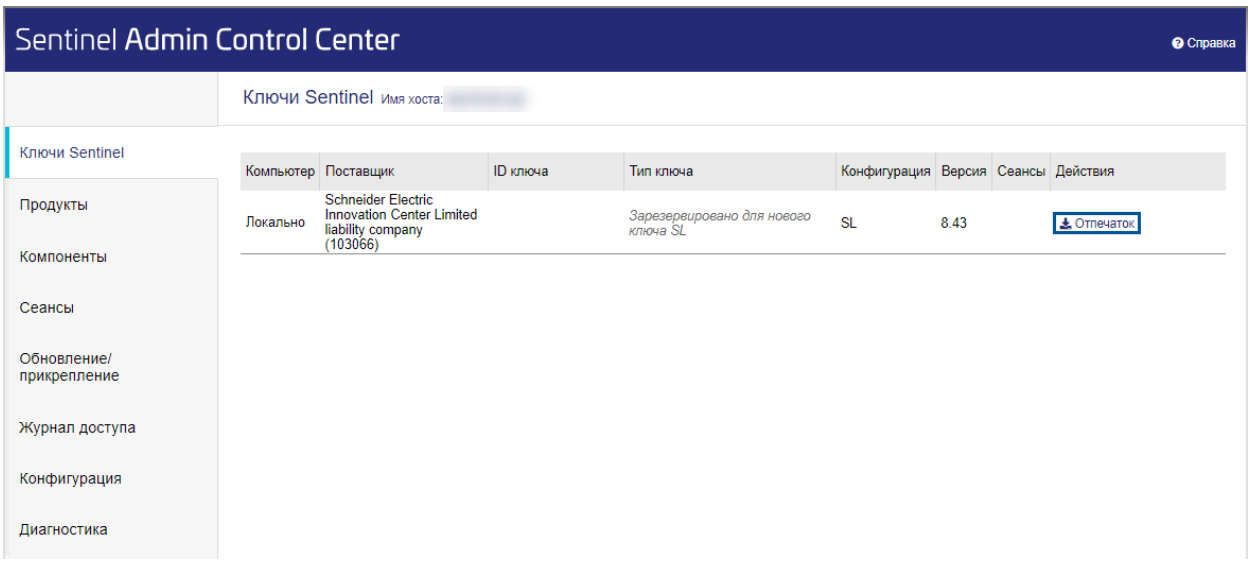
16.2.2.4. Программный ключ Sentinel SL

Активация и обновление набора лицензий программного ключа Sentinel SL выполняется через web-интерфейс **Sentinel Admin Control Center**, который доступен по адресу http://127.0.0.1:1947/ после установки драйвера Sentinel HASP.

> ОБРАТИТЕ ВНИМАНИЕ
>
> Программный ключ Sentinel SL может быть активирован только на одном компьютере.

Активация

1. На компьютере в web-браузере откройте страницу http://127.0.0.1:1947/.
   1.1. В разделе **Ключи Sentinel** для нового ключа SL нажмите кнопку **Отпечаток**.



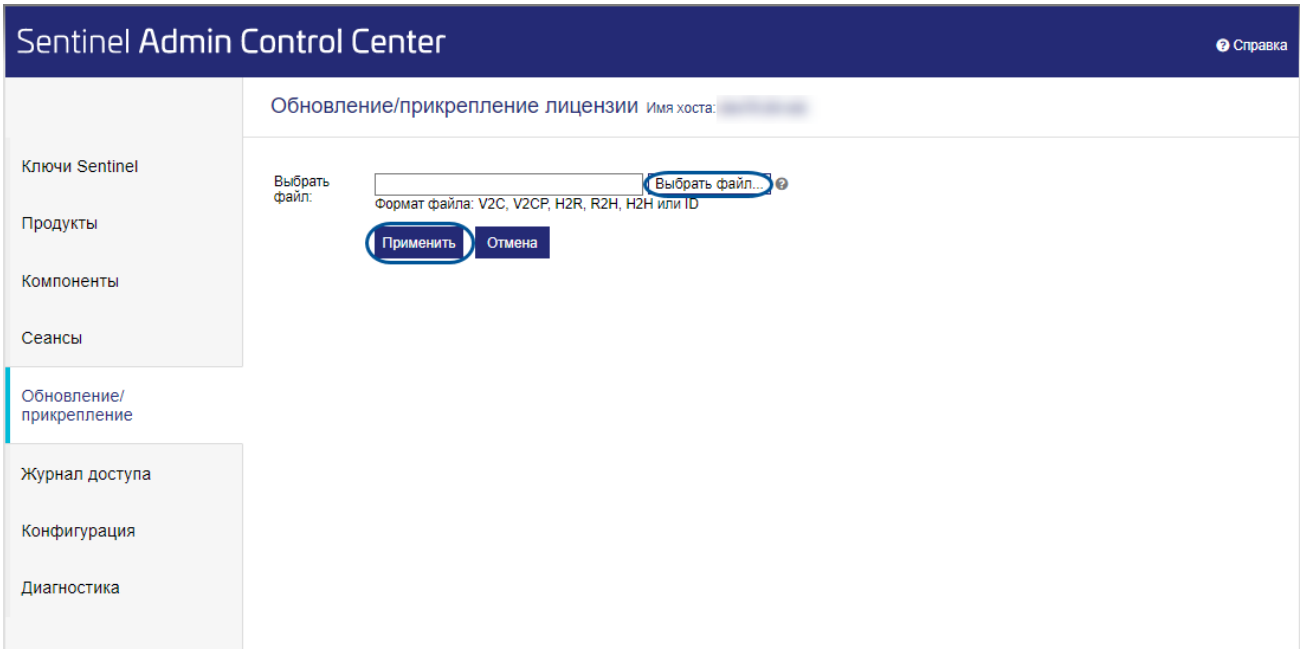
1.2. Сохраните файл формата `*.c2v` на диске.

> ПРИМЕЧАНИЕ
>
> `*.c2v` - **«Customer To Vendor»** - файл образа системы

2. Сгенерированный файл образа системы формата `*.c2v` отправьте на электронную почту `support@systemesoft.ru`. В ответном письме будет выслан файл активации лицензии формата `*.v2c`.

> ПРИМЕЧАНИЕ
>
> `*.v2c` - **«Vendor To Customer»** - файл активации лицензии

3. Перейдите в раздел **Обновление/прикрепление**. Нажмите кнопку **Выбрать файл...**, выберите полученный файл активации лицензии формата `*.v2c` и нажмите кнопку **Применить**.



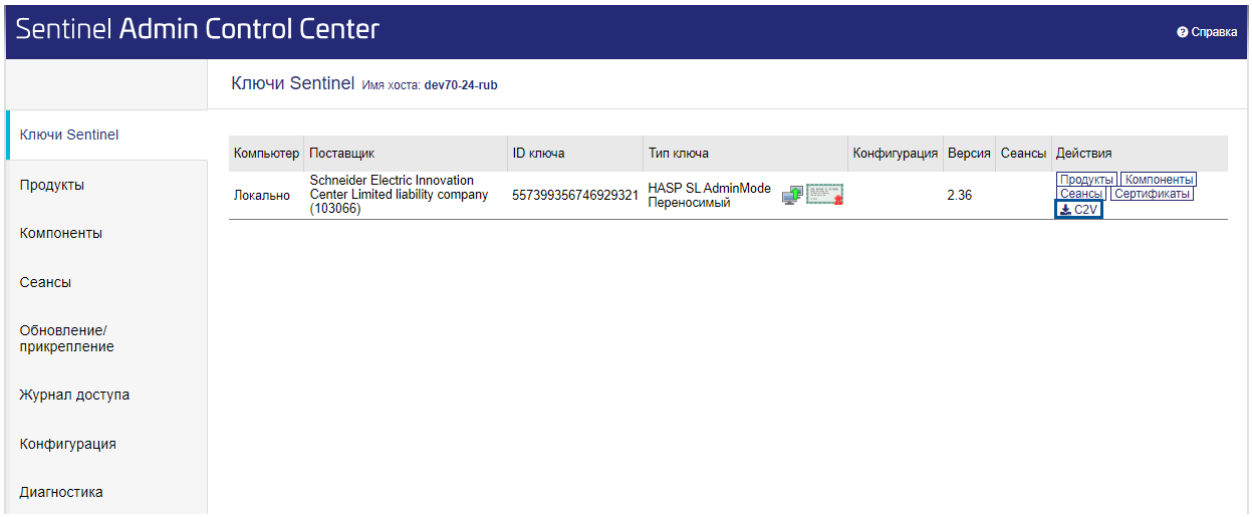
4. Перезапустите сервис **`seplatform.licenseserver.agent`** командой:

```
systemctl restart seplatform.licenseserver.agent
```

После чего программный ключ Sentinel SL будет активирован.

Обновление

1. На компьютере в web-браузере откройте страницу http://127.0.0.1:1947/.
   1.1. В разделе **Ключи Sentinel** для нужного ключа нажмите кнопку **C2V**.



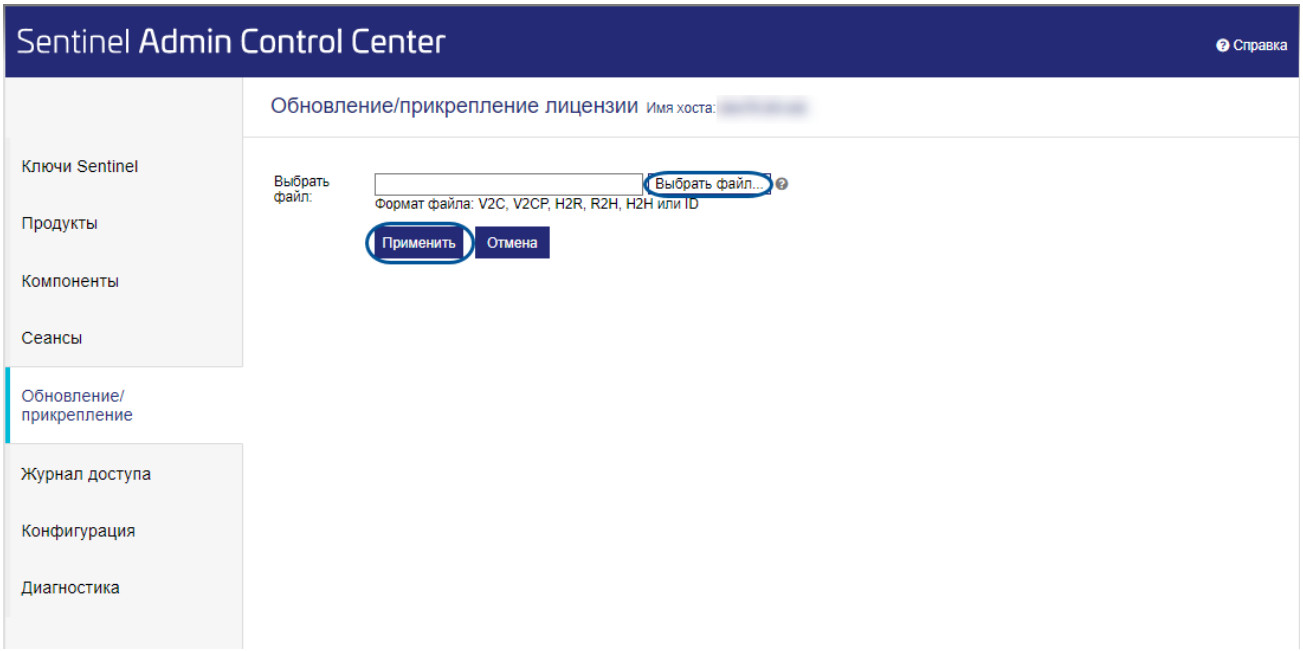
   1.2. Сохраните файл образа ключа формата `*.c2v` на диске.

> ПРИМЕЧАНИЕ
> `*.c2v` - **«Customer To Vendor»** - файл образа ключа

2. Сгенерированный файл образа ключа формата `*.c2v` отправьте на электронную почту `support@systemesoft.ru`. В ответном письме будет выслан файл обновления набора лицензий формата `*.v2c`.

> ПРИМЕЧАНИЕ
> `*.v2c` - **«Vendor To Customer»** - файл набора лицензий

3. Перейдите в раздел **Обновление/прикрепление**. Нажмите кнопку **Выбрать файл...**, выберите полученный файл обновления набора лицензий формата `*.v2c` и нажмите кнопку **Применить**.



4. Перезапустите сервис **seplatform.licenseserver.agent** командой:

```
systemctl restart seplatform.licenseserver.agent
```

После чего набор лицензий программного ключа Sentinel SL будет обновлен.

16.3. Решение проблем

В случае возникновения любых проблем при работе с аппаратными или программными ключами Систэм Платформ отправляйте на адрес электронной почты `support@systemesoft.ru` письмо, содержащее:

- ключ продукта или ID ключа, указанный в сертификате из комплекта поставки;
- описание возникшей проблемы.

17. Безопасное администрирование

Чтобы избежать сбоев в работе компонентов Систэм Платформ и снизить вероятность возникновения уязвимостей проекта автоматизации технологического процесса, следуйте рекомендациям по безопасному администрированию.

Несоблюдение рекомендаций может повлечь:

- потерю технологических данных;
- подачу ложных команд управления технологическому оборудованию;
- возникновение аварийных ситуаций;
- несвоевременное оповещение о наступивших событиях и авариях;
- потерю контроля над ходом технологического процесса;
- остановку технологического оборудования;
- нарушение безопасности производства;
- действие вредоносных программ.

Последствиями могут стать:

- финансовые потери предприятия;
- ситуации, связанные с потерей здоровья и жизни людей;
- техногенные аварии;
- экологические катастрофы.

17.1. Общие рекомендации

Ограничивайте доступ к техническим средствам

Чтобы предотвратить несанкционированный доступ посторонних лиц и негативное воздействие окружающей среды (пыль, влага), рекомендуем размещать технические средства (серверы, АРМ, сетевое оборудование) в серверных шкафах.

Несоблюдение данной рекомендации может привести к прекращению или сбоям в работе компонентов Систэм Платформ в результате:

- отключения оборудования;
- отсоединения кабелей;
- порчи или кражи оборудования;
- прочих физических воздействий, приводящих к отключению или поломке технических средств.

Используйте IPSec

Чтобы предотвратить несанкционированный доступ к сети и перехват пакетов данных, передаваемых по межсетевому протоколу IP, рекомендуем использовать IPSec в туннельном режиме для организации безопасного сетевого взаимодействия между удаленными компонентами Систэм Платформ.

Несоблюдение данной рекомендации несет угрозу перехвата, просмотра, изменения и прочих нежелательных действий с пакетами данных, передаваемыми между удаленными компонентами Систэм Платформ.

Ограничивайте число портов, используемых DCOM

Чтобы предотвратить несанкционированный доступ и повысить безопасность сетевого взаимодействия между удаленными компонентами Систэм Платформ, рекомендуем ограничивать число портов, используемых DCOM, до определенного диапазона. Затем рекомендуем настраивать межсетевой экран (брандмауэр):

- запретить входящий трафик на узел OPC;
- разрешить входящий трафик определенных узлов OPC через порт TCP 135;
- разрешить входящий трафик определенных узлов OPC через некоторый диапазон портов TCP.

Несоблюдение данной рекомендации несет угрозу несанкционированного подключения к сети, сетевых атак, проникновения вредоносных программ и других сетевых угроз, способных вызвать серьезные сбои в работе компонентов Систэм Платформ.

Используйте антивирусное ПО и обновляйте антивирусные базы

Чтобы избежать заражения серверов и АРМ компьютерными вирусами, рекомендуем использовать антивирусное ПО и регулярно обновлять антивирусные базы. Обновление антивирусных баз рекомендуется предварительно выполнять на тестовой платформе ("песочнице").
Совместимым решением для антивирусной защиты станций и серверов с Систэм Платформ является программный продукт Kaspersky Industrial CyberSecurity for Nodes для устройств под управлением ОС Windows и Kaspersky Industrial CyberSecurity for Linux Nodes для устройств под управлением ОС Linux.
Несоблюдение данной рекомендации может привести к серьёзным сбоям в работе компьютеров при заражении вирусами, например:

- внезапная перезагрузка или невозможность включения;
- вывод на экран посторонних сообщений;
- блокировка компьютера;
- замедление работы;
- удаление или изменение файлов приложений;
- форматирование жесткого диска;
- другие непредсказуемые ситуации.

Сбои в работе компьютеров приводят к замедлению, сбоям и прекращению работы компонентов Систэм Платформ.

Отключайте автоматическое обновление ПО

Чтобы избежать сбоев в работе серверов и АРМ, рекомендуем отключать автоматическое обновление ОС и антивирусного ПО.

ОБРАТИТЕ ВНИМАНИЕ

Обновлять ОС, антивирусное ПО, компоненты Систэм Платформ и ПО проекта автоматизации рекомендуем во время плановых работ по техническому обслуживанию и ремонту.

Несоблюдение данной рекомендации повышает вероятность сбоя в работе компонентов Систэм Платформ.

Блокируйте доступ к информации на внешнем накопителе

Чтобы предотвратить несанкционированное использование внешних накопителей, рекомендуем блокировать порты USB и приводы оптических дисков для учетных записей пользователей.

ПРИМЕЧАНИЕ

Подключив к системному блоку внешний накопитель, пользователь не увидит его в папке `Мой компьютер` или доступ к нему будет запрещён.

Несоблюдение данной рекомендации может привести к заражению компьютеров вредоносными программами, содержащимися на накопителях, а также утечке конфиденциальной информации предприятия.

Ограничивайте права и количество учетных записей пользователей

Чтобы предотвратить несанкционированный доступ к ПО серверов и АРМ, рекомендуем включать только учетные записи пользователей, предусмотренные проектом автоматизации. Для каждой учетной записи:

- устанавливайте сложные пароли;
- ограничивайте права пользователя в использовании ПО рамками должностных обязанностей.

Несоблюдение данной рекомендации несет угрозу несанкционированного доступа к ПО пользователей, не обладающих необходимыми знаниями, что может привести к ошибкам в работе с ПО, компонентами Систэм Платформ и управлении технологическим процессом.

Минимальные права учётной записи для запуска компонентов Систэм Платформ

Приложения и службы выполняются с правами учётной записи, от имени которой они запущены:

- Приложения запускаются от имени учётной записи пользователя, запустившего приложение.
- Службы по умолчанию запускаются от имени системной учётной записи LocalSystem - это специальная учётная запись, которую создаёт система. Для каждой службы можно изменить учётную запись, от имени которой она запускается (стр. 108).

Системная учётная запись обладает полными правами в системе. Права прочих учётных записей определяются системными группами пользователей, в которую эти учётные записи включены: Пользователи, Опытные пользователи, Администраторы и другие.

В таблице ниже для приложений и служб Систэм Платформ приведены требования к правам учётной записи, чтобы запущенное от её имени приложение/служба могли выполнять свои функции.

Компонент	**Минимальные права учётной записи**
SePlatform.Data Server SePlatform.AccessPoint	Для службы - системная учётная запись. Для сервисных приложений - Пользователь.
SePlatform.Historian	Системная учётная запись.
SePlatform.Development Studio	Пользователь.
SePlatform.HMI	Пользователь.
SePlatform.Mapping Server	Сетевая служба (NetworkService).

Компонент	Минимальные права учётной записи
SePlatform.Security	Пользователь. Для конфигурирования - Администратор.

Изменение учётной записи, от имени которой запускается служба

ОС Windows

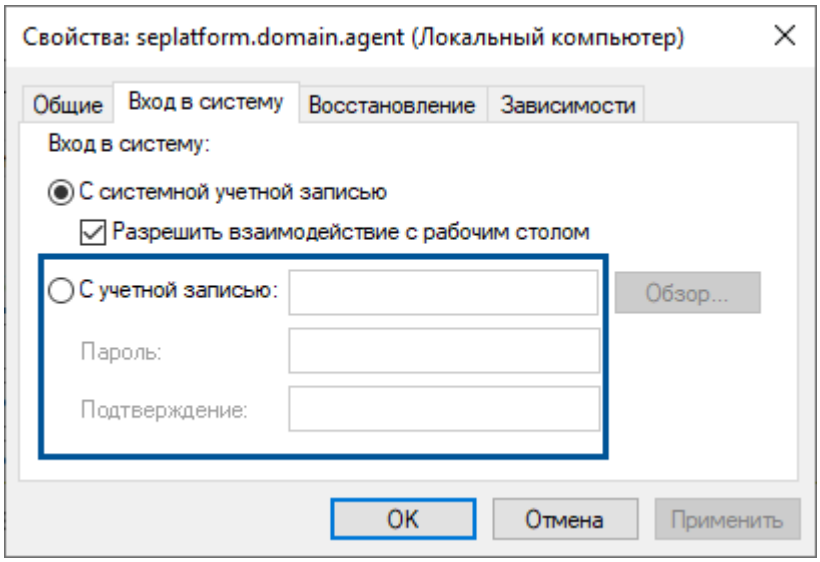
1. Откройте список служб.

Сделать это можно:

- в диспетчере задач на вкладке **Службы**
- открыть окно запуска **«Win»** + **«R»** и ввести

```
services.msc
```

2. В списке выберите службу и в контекстном меню откройте её свойства.
3. На вкладке **Вход в систему** укажите учётную запись, от имени которой служба будет исполняться.



ОБРАТИТЕ ВНИМАНИЕ

Если пароль пользователя впоследствии изменится, в свойствах службы он не обновится: потребуется повторно зайти в свойства службы и изменить пароль пользователя.

4. Чтобы изменения вступили в силу, перезапустите службу.

ОБРАТИТЕ ВНИМАНИЕ

Выполненные настройки сбрасываются при удалении или переустановке. Поэтому описанную выше настройку нужно выполнять после каждой установки; например, после установки более новой версии.

ОС Linux

Сервисы компонентов Систэм Платформ по умолчанию запускаются от имени суперпользователя **«root»**. Для сервисов SePlatform.Data Server, SePlatform.AccessPoint, SePlatform.Domain, агента SePlatform.License Server, SePlatform.Historian, SePlatform.Security и приложений SePlatform.HMI,

SePlatform.HMI.Alarms, SePlatform.HMI.Trends возможно переназначить пользователя, от имени которого будет запускаться сервис/приложение.

ОБРАТИТЕ ВНИМАНИЕ

Для работы SePlatform.Mapping Server права суперпользователя **«root»** не требуются.

Смена пользователя для сервиса SePlatform.Security описана в документации на SePlatform.Security.

Чтобы сменить пользователя для сервисов SePlatform.Data Server, SePlatform.AccessPoint и SePlatform.Domain, используйте следующую инструкцию.

ОБРАТИТЕ ВНИМАНИЕ

Ниже приведена инструкция по настройке запуска сервисов от имени непривилегированного пользователя, актуальная для версии SePlatform.Domain 1.2.8 и новее. Если вы используете более раннюю версию, вам понадобится инструкция, описанная в документации для SePlatform.Domain, соответствующей используемой вами версии.

1. Если пользователь, от имени которого необходимо запускать сервисы, присутствует в системе, перейдите к следующему шагу. Если пользователя не существует - создайте его с помощью команды `useradd`. Используйте модификатор `-m`, чтобы создать папку пользователя. Имя пользователя может быть любым.

```
sudo useradd -m имя_пользователя
```

Настройте для созданного пользователя фоновое присутствие в системе.

```
sudo loginctl enable-linger имя_пользователя
```

Текущее состояние присутствия пользователя можно проверить по команде:

```
sudo loginctl show-user имя_пользователя
```

Присутствие пользователя описано строкой `Linger=yes` в возвращаемом результате, отсутствие - ошибкой выполнения команды `Failed to get user: User ID xxxx is not logged in or lingering`.

Затем задайте пароль для созданного пользователя при помощи команды `passwd` (если не был задан при создании пользователя):

```
sudo passwd имя_пользователя
```

2. Остановите и запретите работу сервисов, по умолчанию запускаемых от имени суперпользователя root.

```
sudo systemctl stop seplatform.domain
sudo systemctl disable seplatform.domain
sudo systemctl stop seplatform.net
sudo systemctl disable seplatform.net
sudo systemctl stop seplatform.accesspoint
sudo systemctl disable seplatform.accesspoint
sudo systemctl stop seplatform.server
sudo systemctl disable seplatform.server
```

3. Измените номер порта Net-агента на значение выше 10000 (например, 11010). Это необходимо, потому что непривилегированным пользователям нельзя "прослушивать" порты с малыми номерами. Для этого:

3.1. Перейдите к папке, где хранятся конфигурационные файлы SePlatform.Domain - `/opt/SePlatform/SePlatform.Domain`. Укажите новое значение порта в конфигурационных файлах `seplatform.net.agent.xml` и `seplatform.domain.agent.xml`.

3.2. Если используете SePlatform.Security, не забудьте указать новое значение порта для агента безопасности. Для этого перейдите к папке, где хранятся конфигурационные файлы агента безопасности - `/opt/SePlatform/SePlatform.Security`. Замените в конфигурационном файле `seplatform.security.agent.xml` номер порта Net-агента на новое значение.

4. Укажите имя непривилегированного пользователя вместо идентификатора root в следующих юнит-файлах:

- `/lib/systemd/system/seplatform.domain.service`;
- `/lib/systemd/system/seplatform.net.service`;
- `/lib/systemd/system/seplatform.server.service`;
- `/lib/systemd/system/seplatform.accesspoint.service`.

ПРИМЕР

Вместо

```
User=root
Group=root
```

укажите

```
User=имя_пользователя
Group=группа_пользователя
```

5. Скопируйте файл `server_launcher.sh` из папки установки SePlatform.Domain в папки установки SePlatform.Data Server и SePlatform.AccessPoint.

```
sudo cp /opt/SePlatform/SePlatform.Domain/server_launcher.sh
/opt/SePlatform/SePlatform.Server
sudo cp /opt/SePlatform/SePlatform.Domain/server_launcher.sh
/opt/SePlatform/SePlatform.AccessPoint
```

6. Создайте символическую ссылку на скопированный файл в формате `*.xml`:

- для SePlatform.Data Server:

```
cd /opt/SePlatform/SePlatform.Server
sudo ln -s SePlatform.Data Server.xml server_launcher.sh.xml
```

- для SePlatform.AccessPoint:

```
cd /opt/SePlatform/SePlatform.AccessPoint
sudo ln -s SePlatform.AccessPoint.xml server_launcher.sh.xml
```

7. Измените юнит-файлы сервисов служб SePlatform.Data Server и SePlatform.AccessPoint. Укажите в файлах полный путь к скопированному файлу `server_launcher.sh` в строке запуска `ExecStart`. Остальную часть строки оставьте без изменений.

- В юнит-файле `/lib/systemd/system/seplatform.server.service` вместо:

```
ExecStart=/opt/SePlatform/SePlatform.Server/SePlatform.Server 1>/dev/null &
```

укажите:

```
ExecStart=/opt/SePlatform/SePlatform.Server/server_launcher.sh
/opt/SePlatform/SePlatform.Server/SePlatform.Server 1>/dev/null &
```

- В юнит-файле `/lib/systemd/system/seplatform.accesspoint.service` вместо:

```
ExecStart=/opt/SePlatform/SePlatform.AccessPoint/SePlatform.AccessPoint -accesspoint
1>/dev/null &
```

укажите:

```
ExecStart=/opt/SePlatform/SePlatform.AccessPoint/server_launcher.sh
/opt/SePlatform/SePlatform.AccessPoint/SePlatform.AccessPoint -accesspoint
1>/dev/null &
```

8. Измените владельца папок установки SePlatform.Domain, SePlatform.AccessPoint и SePlatform.Data Server вместе с их содержимым. Это необходимо, чтобы для пользователя не возникало ошибки доступа к указанным папкам.

```
sudo chown -R имя_пользователя:группа_
пользователя/opt/SePlatform/SePlatform.Domain
sudo chown -R имя_пользователя:группа_
пользователя/opt/SePlatform/SePlatform.Server
sudo chown -R имя_пользователя:группа_
пользователя/opt/SePlatform/SePlatform.AccessPoint
```

9. В конфигурационном файле Domain-агента укажите папку для хранения временных конфигураций (кэша), к которой у пользователя есть доступ. Для этого перейдите к папке, где хранятся конфигурационные файлы SePlatform.Domain - `/opt/SePlatform/SePlatform.Domain`. В конфигурационном файле `seplatform.domain.agent.xml` укажите полный путь к подходящей папке в качестве значения атрибута `<StoragePath>` xml-элемента `<Components>`, например, `/home/newuser/DomainStorage/cache/server`.

10. Откройте файл `/opt/SePlatform/SePlatform.Server/SePlatform.Data Server.xml` и добавьте строку **«<Config ReadOnly="True"/>»**:

```
<configuration>
<install ServiceName="SePlatform.Server" ExeName="SePlatform.Server.exe" />
<Storage Filename="SePlatformServer.cfg" />
<Connection Port="4572" />
<Backup Path="..\Backups" Time="00:00" StorageDepth="14" />
<Log Path="..\Logs" />
<Dispatch Model="Default" />
<Config ReadOnly="True" />
<Instance ID="9F4443FA-ADD2-42F0-9AB7-BD906DDA238F" />
</configuration>
```

Такая настройка запрещает редактировать конфигурацию SePlatform.Data Server через сервисное приложение Конфигуратор. Возможность открытия и просмотра конфигурации в Конфигураторе при этом остаётся.

11. Запустите все отключенные ранее сервисы и разрешите их работу:

```
sudo systemctl start seplatform.domain
sudo systemctl enable seplatform.domain
sudo systemctl start seplatform.net
sudo systemctl enable seplatform.net
sudo systemctl start seplatform.accesspoint
sudo systemctl enable seplatform.accesspoint
sudo systemctl start seplatform.server
sudo systemctl enable seplatform.server
```

12. Теперь следует перезагрузить операционную систему. После этого следует убедиться, что сервисы запущены от имени непривилегированного пользователя, выполнив команду `ps aux`. Чтобы отфильтровать информацию, предоставляемую командой, используйте фильтр `grep`:

```
ps aux | grep seplatform
```

Чтобы сменить пользователя для сервиса агента SePlatform.License Server:

1. Откройте файл `/lib/systemd/system/seplatform.licensing.agent.service`
2. В строках

```
User=root
Group=root
```

измените **«root»** на нужного пользователя и группу (например, на пользователя/группу с пониженными привилегиями).

3. Чтобы применить измененную конфигурацию, выполните команду:

```
sudo systemctl daemon-reload
```

> ОБРАТИТЕ ВНИМАНИЕ
>
> Ключи Guardant будут работать под пользователем, отличным от **«root»**, только после установки правил доступа к файлу устройства (USB-ключу). Чтобы установить правила, установите Guardant Control Center. После установки отсоедините USB-ключ от порта компьютера и подсоедините его снова.
>
> Если после установки Guardant Control Center ваш ключ по-прежнему не виден в системе, настройте правила вручную (настройка описана в официальной документации Guardant: https://dev.guardant.ru/pages/viewpage.action?pageId=1278017).

Чтобы сменить пользователя для сервиса SePlatform.Historian:

1. Откройте файл `/lib/systemd/system/seplatform-server.service`.
2. В строках

```
User=root
Group=root
```

измените **«root»** на нужного пользователя и группу (например, на пользователя/группу с пониженными привилегиями).

3. Чтобы применить измененную конфигурацию, выполните команду:

```
sudo systemctl daemon-reload
```

4. Назначьте указанного выше пользователя владельцем папки с базой данных и папки с очередью данных. Для этого выполните команды:

```
sudo chown -R <user>:<group> <DatabasePath> (для папки с базой данных)
sudo chown -R <user>:<group> <FileQueuePath> (для папки с очередью данных)
```

Чтобы сменить пользователя для SePlatform.HMI, SePlatform.HMI.Alarms и SePlatform.HMI.Trends достаточно самостоятельно запустить компонент от нужного пользователя. Для корректной работы проекта SePlatform.HMI назначьте выбранного пользователя владельцем папки, в которой хранится проект. Для назначения владельца папки выполните команду:

```
sudo chown -R <user>:<group> <ProjectPath>
```

Ограничивайте права доступа к системным папкам

Чтобы предотвратить несанкционированный доступ к файлам ОС и компонентов Систэм Платформ, рекомендуем ограничивать права доступа к системным папкам.

> ВАЖНО
>
> Не рекомендуем изменять права доступа к каталогам, в которые устанавливаются компоненты Систэм Платформ.

ОБРАТИТЕ ВНИМАНИЕ

Дистрибутивы компонентов Систэм Платформ не изменяют стандартные права доступа к системным каталогам.

Несоблюдение данной рекомендации несет угрозу подмены компонентов Систэм Платформ вредоносными программами, что может привести к серьёзным сбоям в работе проекта автоматизации и всего технологического процесса.

17.2. Рекомендации, применимые для компонентов Систэм Платформ

Используйте системы контроля версий

Чтобы избежать утраты исходных файлов ПО проекта автоматизации, рекомендуем использовать системы контроля версий для хранения и контроля версионности исходных файлов проектов SePlatform.Development Studio и SePlatform.HMI.

Несоблюдение данной рекомендации повышает риск использования устаревших версий исходных файлов проекта автоматизации для доработок и корректировок.

Используйте пароли для доступа к SePlatform.Data Server и SePlatform.AccessPoint

Чтобы предотвратить несанкционированный доступ из сервисных приложений Конфигуратор, Статистика и Управляющий, настоятельно рекомендуем использовать пароли для доступа к SePlatform.Data Server и SePlatform.AccessPoint.

Несоблюдение данной рекомендации несет угрозу несанкционированных действий:

- изменение конфигураций;
- просмотр статистики;
- управление сервером или резервной парой серверов;
- несанкционированный обмен данными.

Несанкционированный доступ и действия могут стать причиной серьёзных сбоев в работе компонентов Систэм Платформ, проекта автоматизации и всего технологического процесса.

18. Правила брандмауэра

Для корректной работы компонентов Систэм Платформ в системе, где используется брандмауэр, необходимо настроить правила для входящих и исходящих подключений.

В правилах для входящих подключений следует разрешить подключения к портам, через которые компоненты Систэм Платформ получают данные.

В правилах для исходящих подключений следует разрешить подключения к портам, через которые компоненты Систэм Платформ отправляют данные.

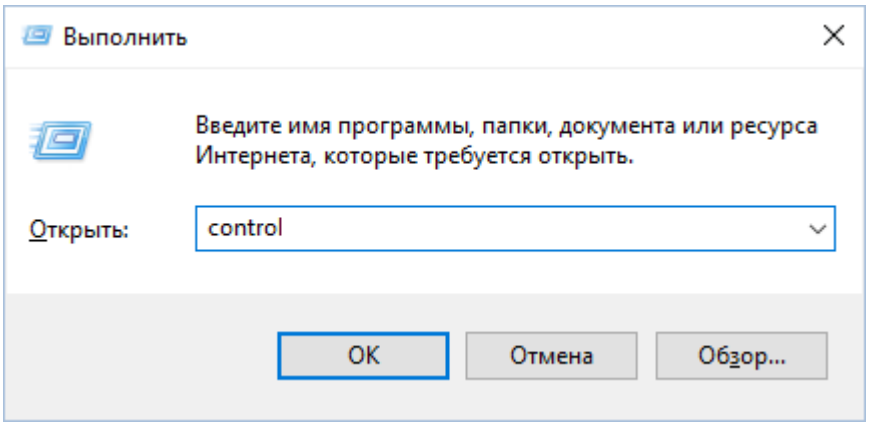
18.1. ОС Windows

ОБРАТИТЕ ВНИМАНИЕ

Настройку правил встроенного брандмауэра Windows следует выполнять только если данный брандмауэр включен и используется в системе. Если в системе используется сторонний брандмауэр, то настройку правил следует выполнять в нём.

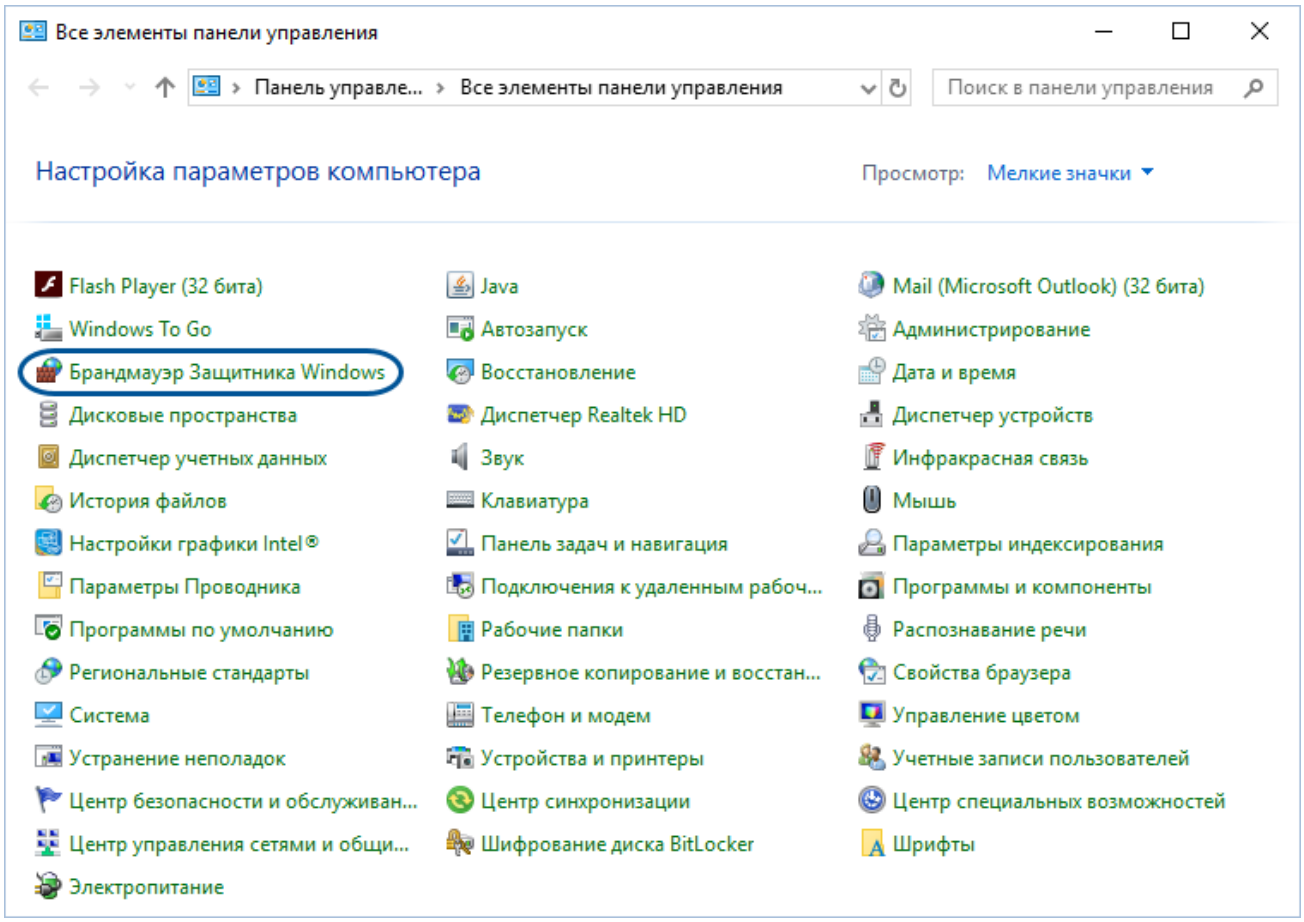
Чтобы настроить правила встроенного брандмауэра Windows:

1. Вызовите меню **Выполнить** комбинацией клавиш **«Windows»+«R»**, введите команду control и нажмите кнопку **OK**.

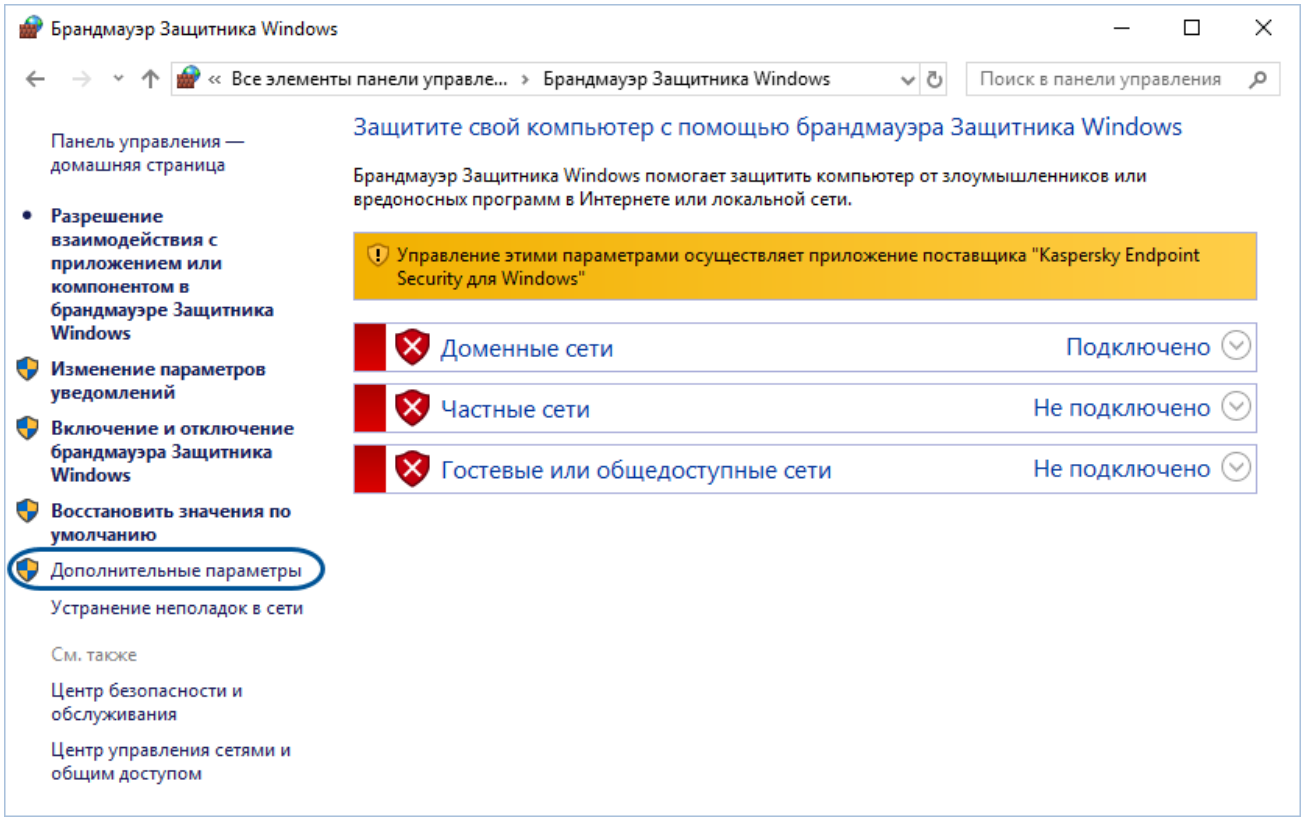


Либо пройдите по пути `Пуск → Служебные → Панель управления → Брандмауэр Защитника Windows`.

2. В открывшемся окне элементов панели управления выберите элемент **Брандмауэр Защитника Windows**.



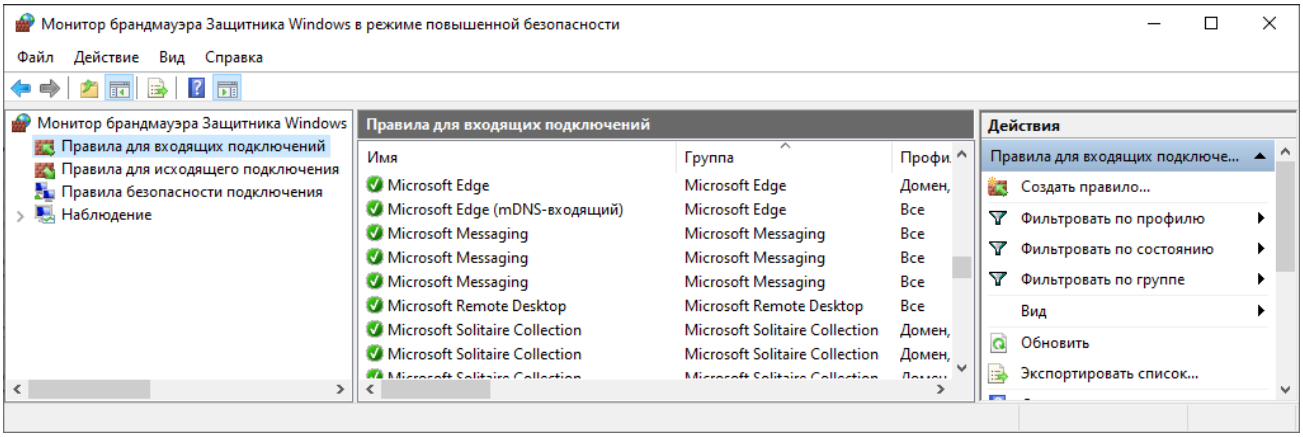
3. В окне **Брандмауэр Защитника Windows** выберите пункт **Дополнительные параметры**.



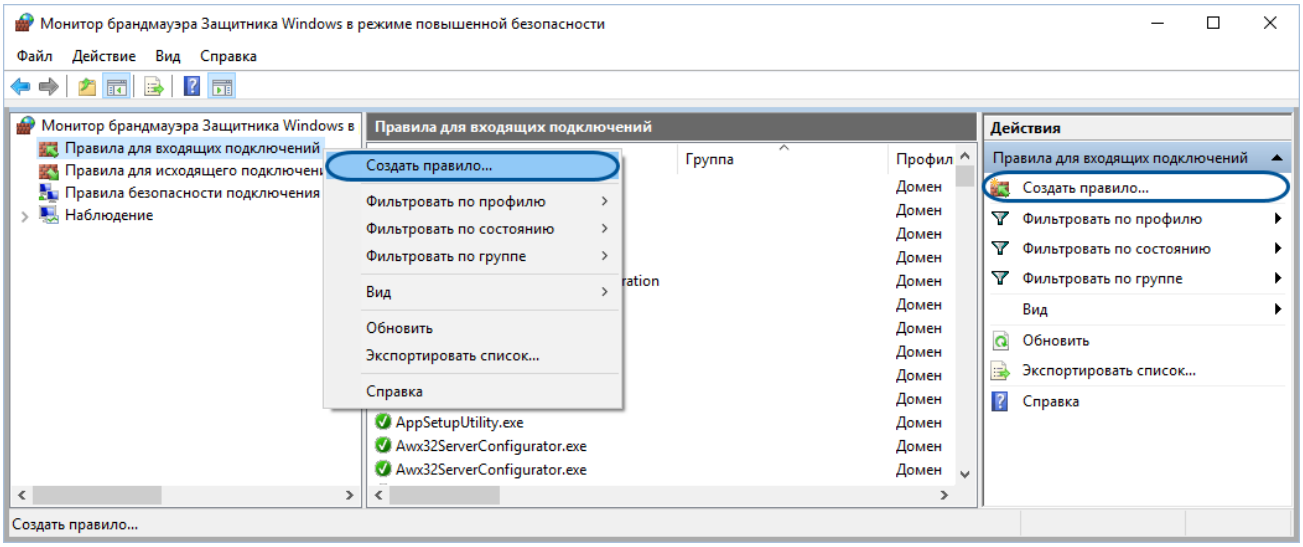
18.1.1. Правила для входящих подключений

Чтобы настроить правила для входящих подключений:

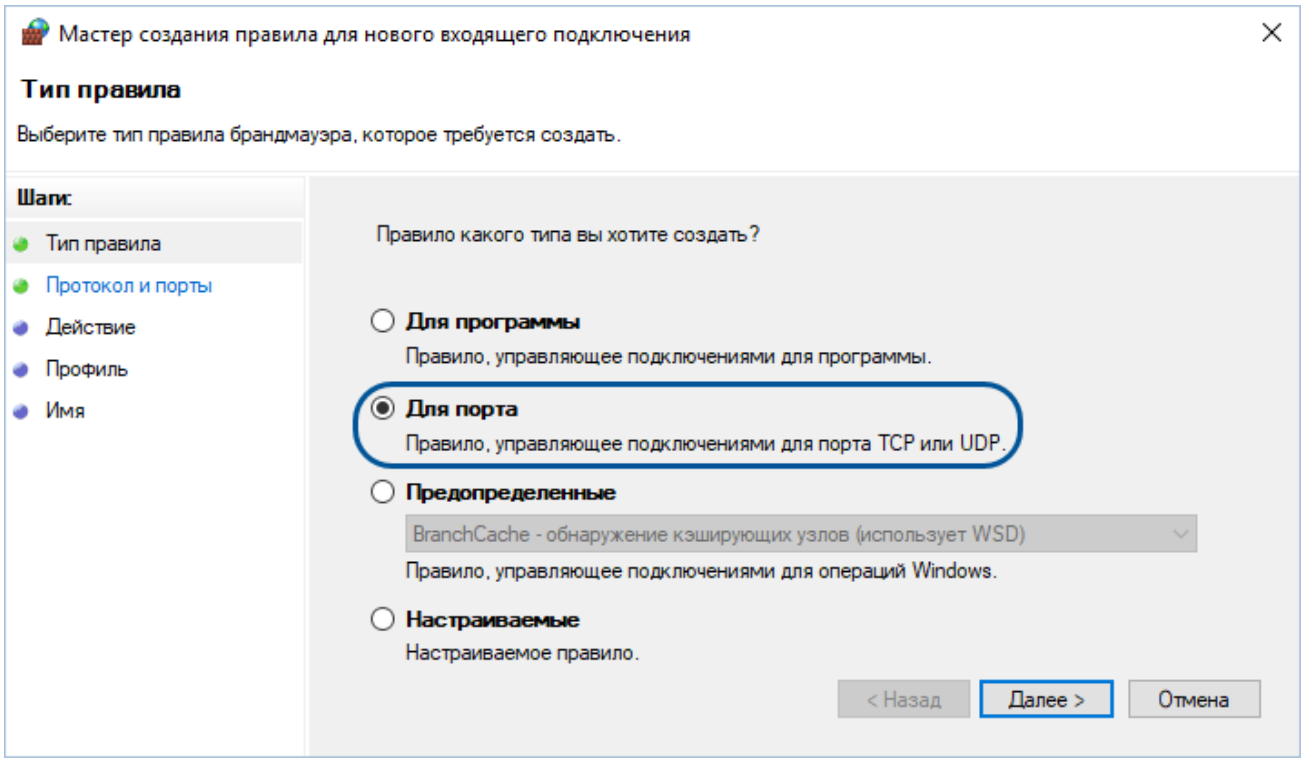
1. В окне **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности** выберите пункт **Правила для входящих подключений**.



2. В контекстном меню или в области **Действия** выберите пункт **Создать правило...**.

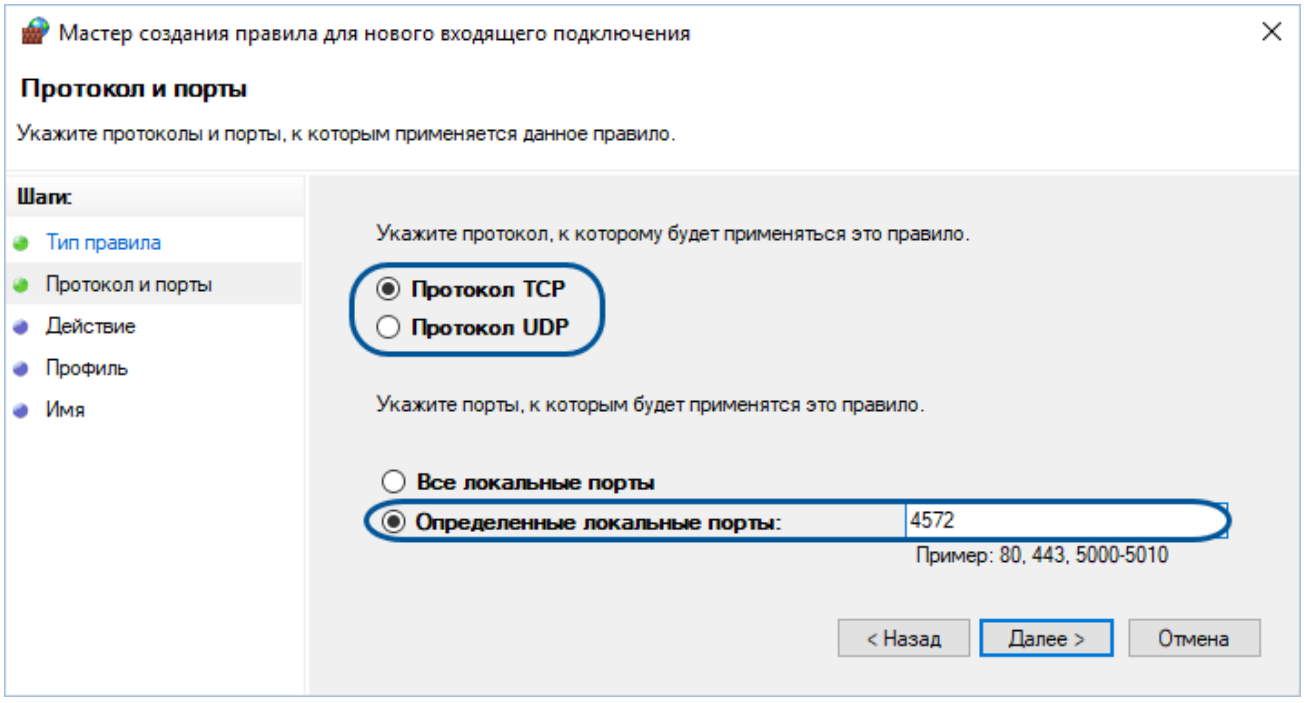


3. В окне **Мастер создания правила для нового входящего подключения** выберите тип подключения **«Для порта»** и нажмите кнопку **Далее**.

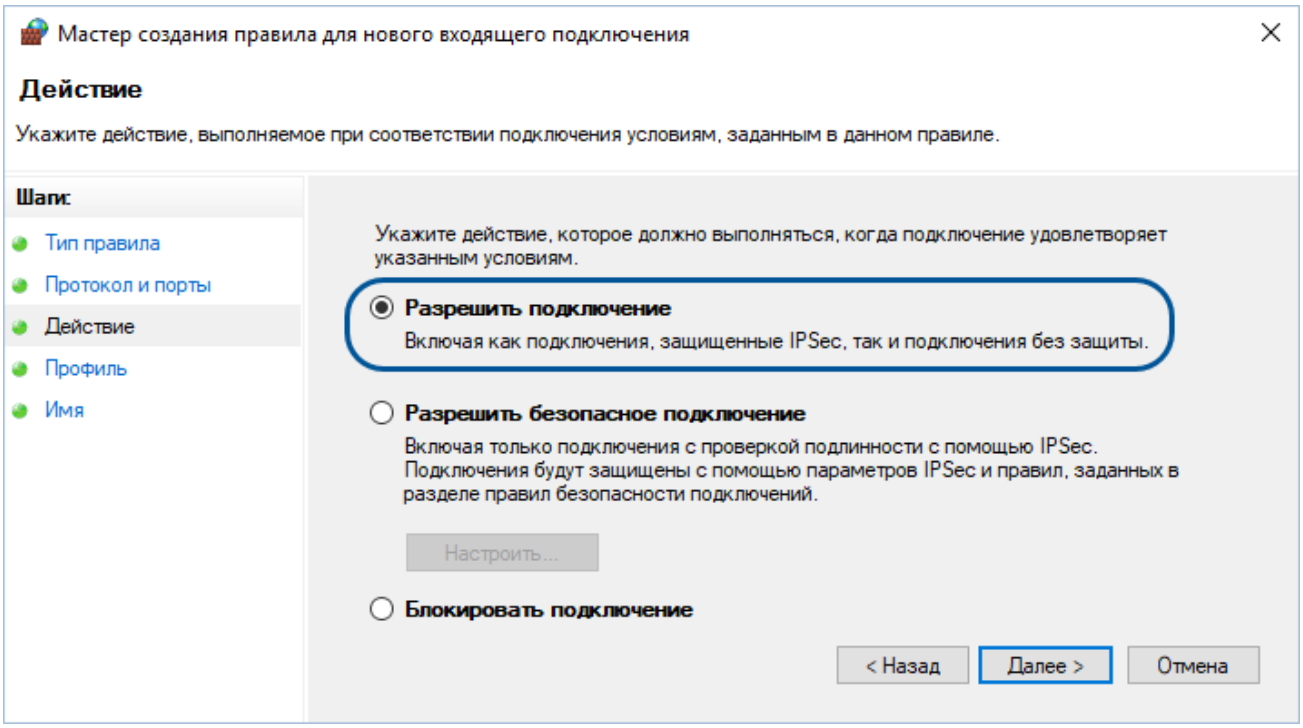


4. Выберите протокол, укажите порты, для которых требуется разрешить подключение и нажмите кнопку **Далее**.

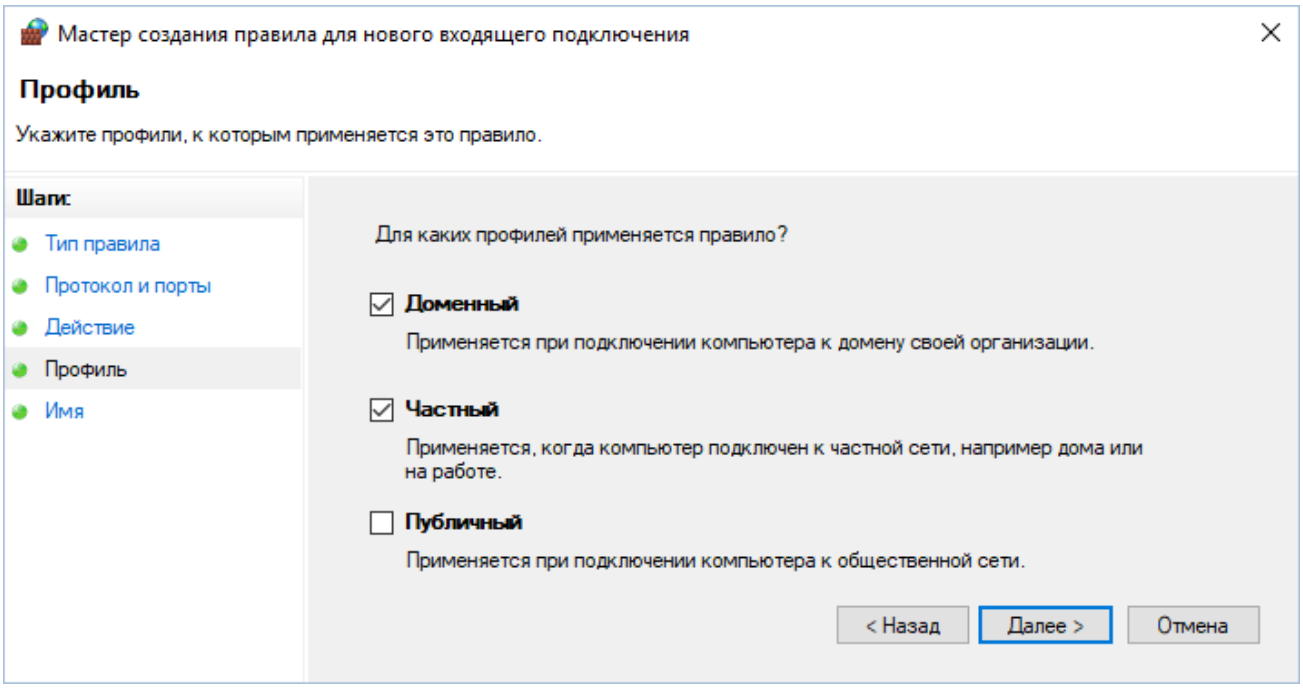
> ОБРАТИТЕ ВНИМАНИЕ
>
> Протоколы и порты, используемые компонентами Систэм Платформ для входящих подключений, приведены в разделе Порты для входящих подключений (см. стр. 125).



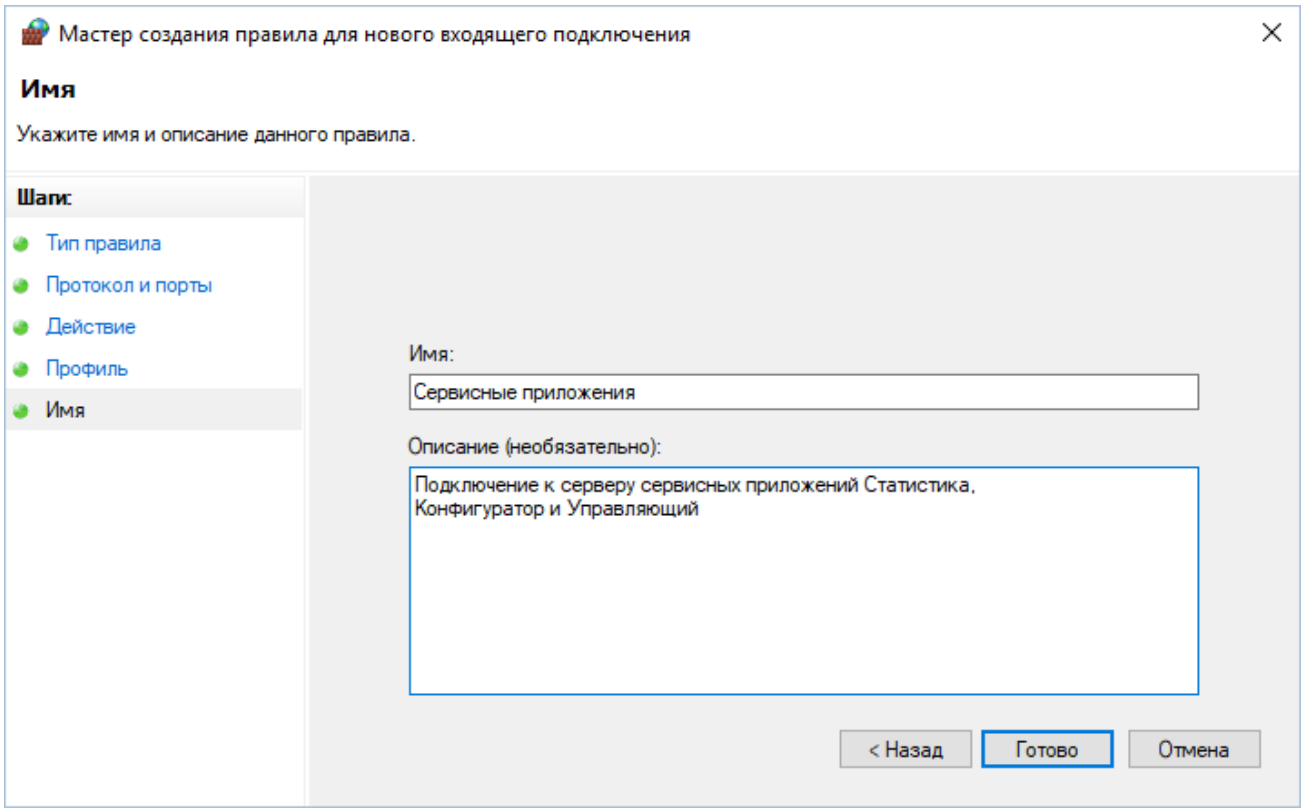
5. Выберите действие **Разрешить подключение** и нажмите кнопку **Далее**.



6. Укажите профили, к которым будет применяться правило, установив соответствующие флаги, и нажмите кнопку **Далее**.



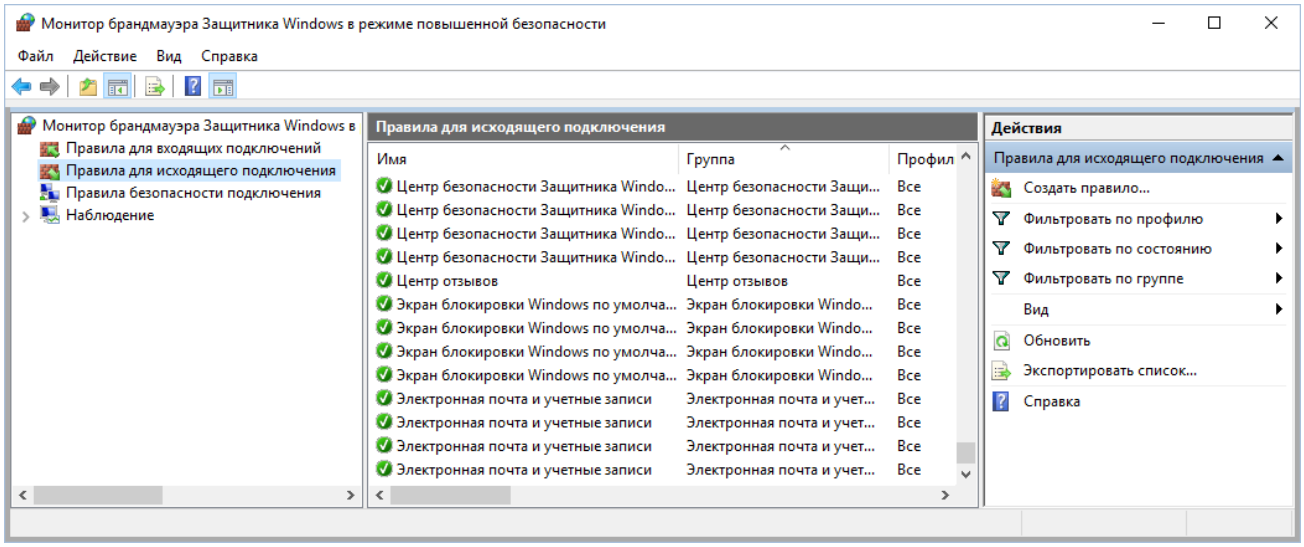
7. Укажите для создаваемого правила имя, описание и нажмите кнопку **Готово**.



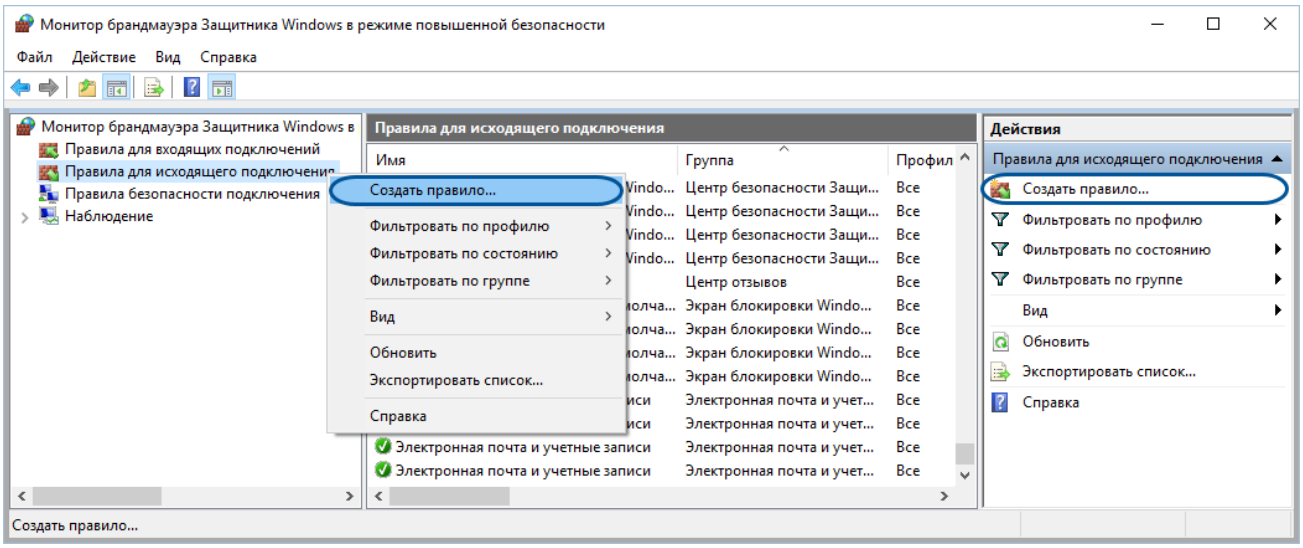
18.1.2. Правила для исходящих подключений

Чтобы настроить правила для исходящих подключений:

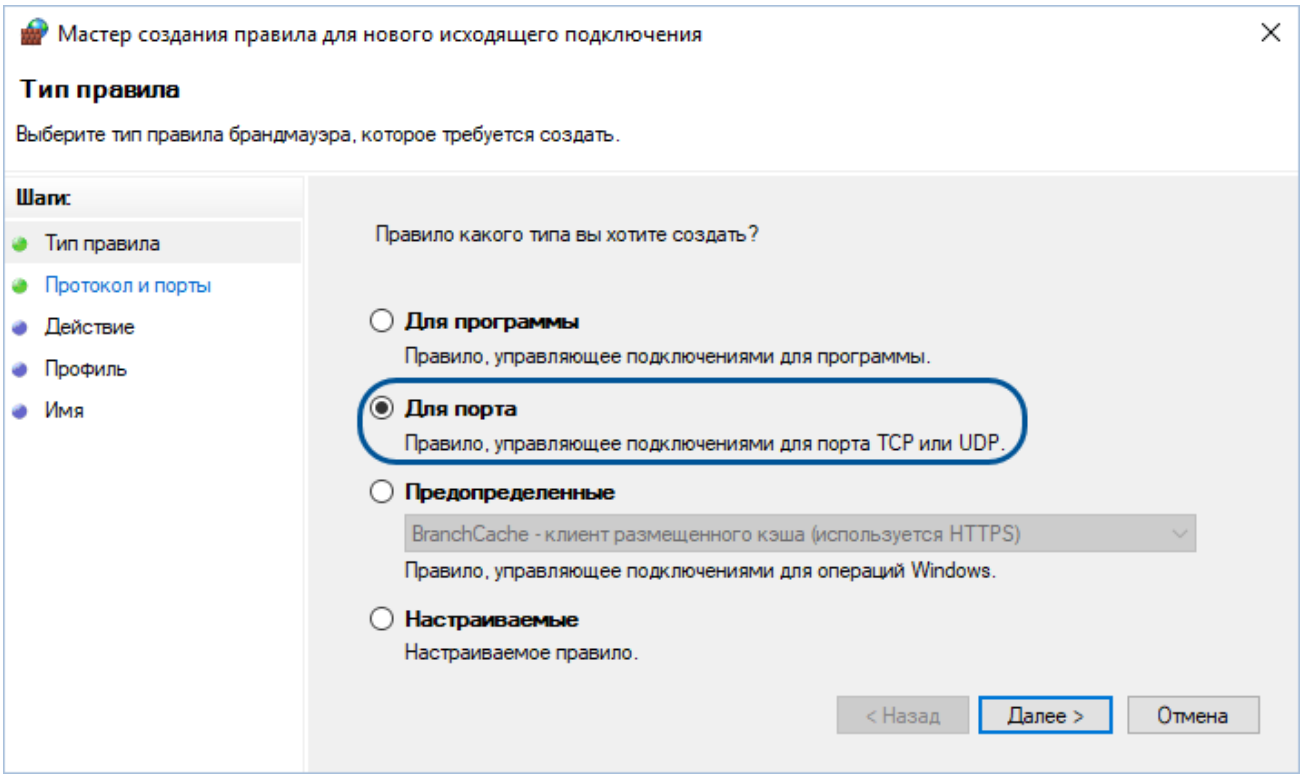
1. В окне **Монитор брандмауэра Защитника Windows в режиме повышенной безопасности** выберите пункт **Правила для исходящего подключения**.



2. В контекстном меню или в области **Действия** выберите пункт **Создать правило...**.



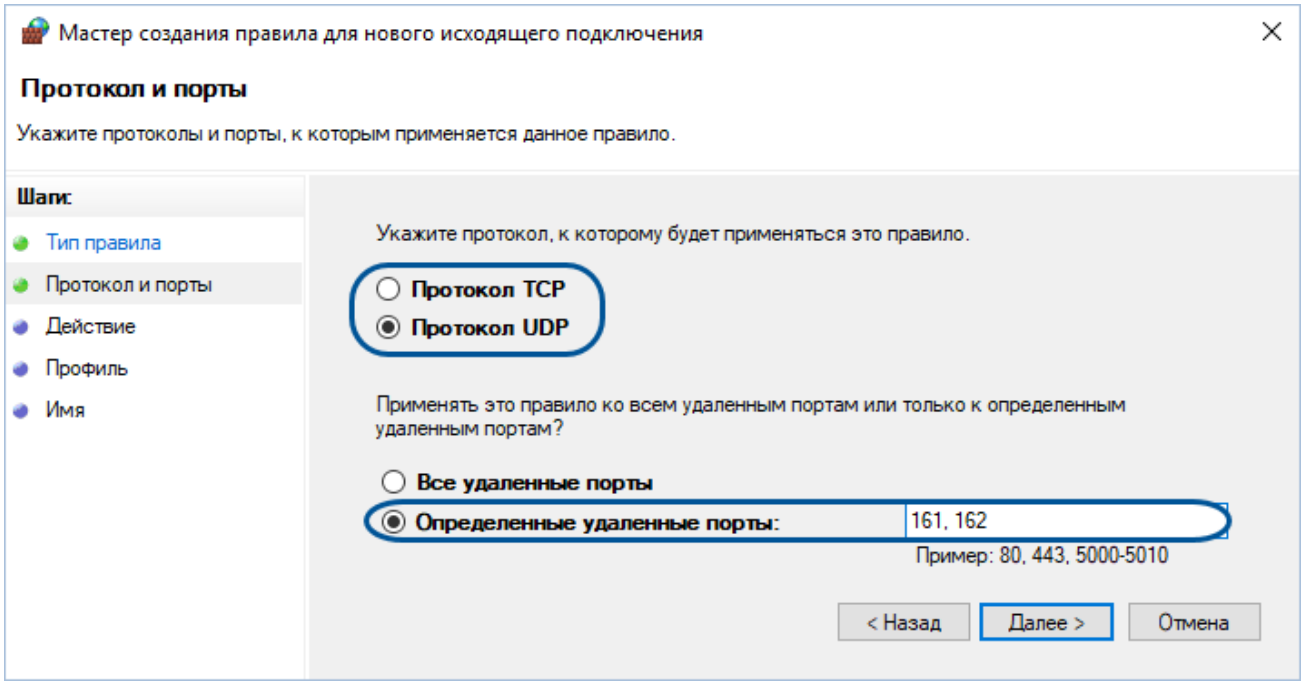
3. В окне **Мастер создания правила для нового исходящего подключения** выберите тип подключения **«Для порта»** и нажмите кнопку **Далее**.



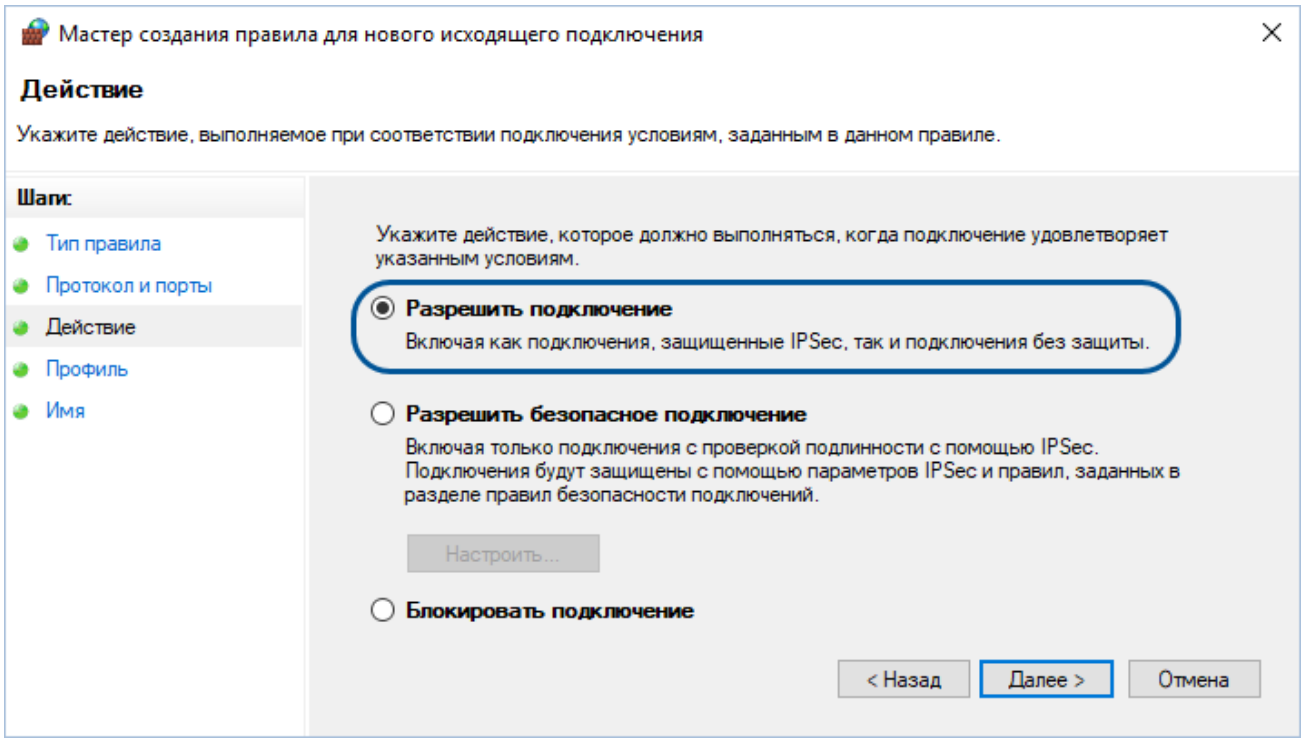
4. Выберите протокол, укажите порты, для которых требуется разрешить подключение и нажмите кнопку **Далее**.

ОБРАТИТЕ ВНИМАНИЕ

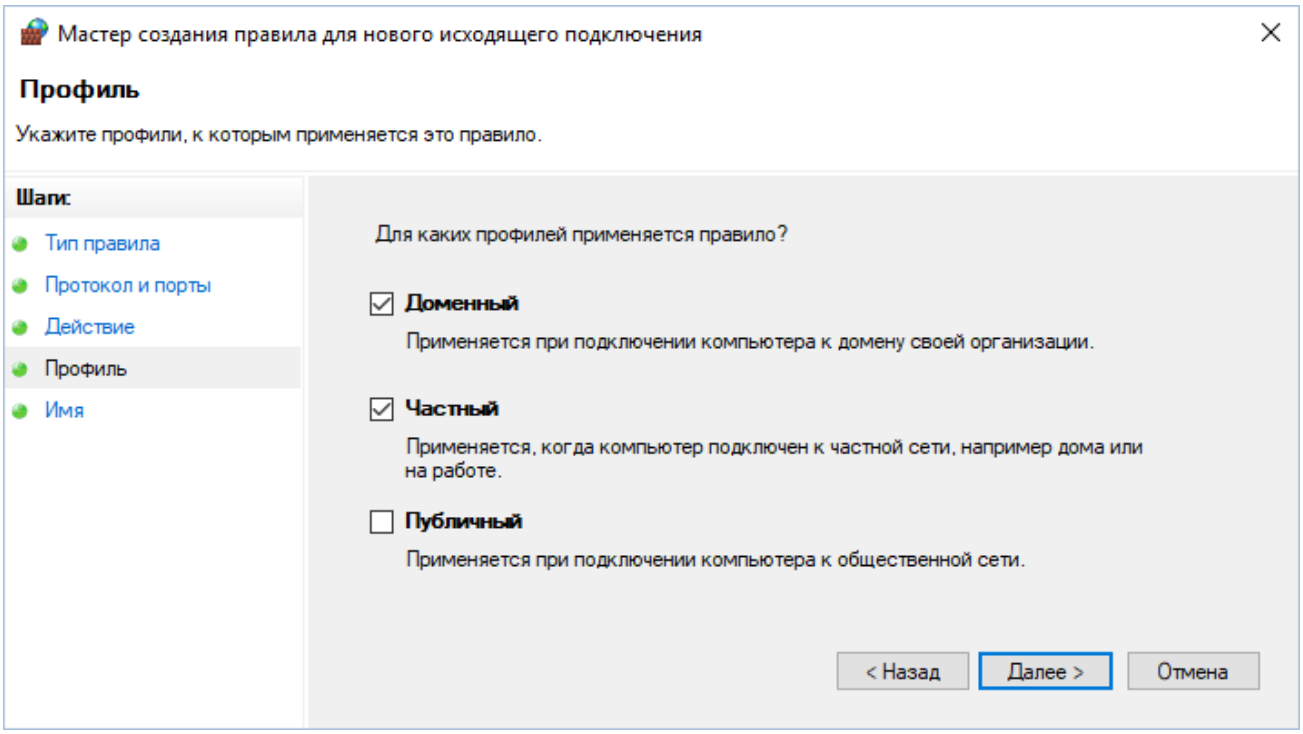
Протоколы и порты, используемые компонентами Систэм Платформ для исходящих подключений, приведены в разделе Порты для исходящих подключений (см. стр. 126).



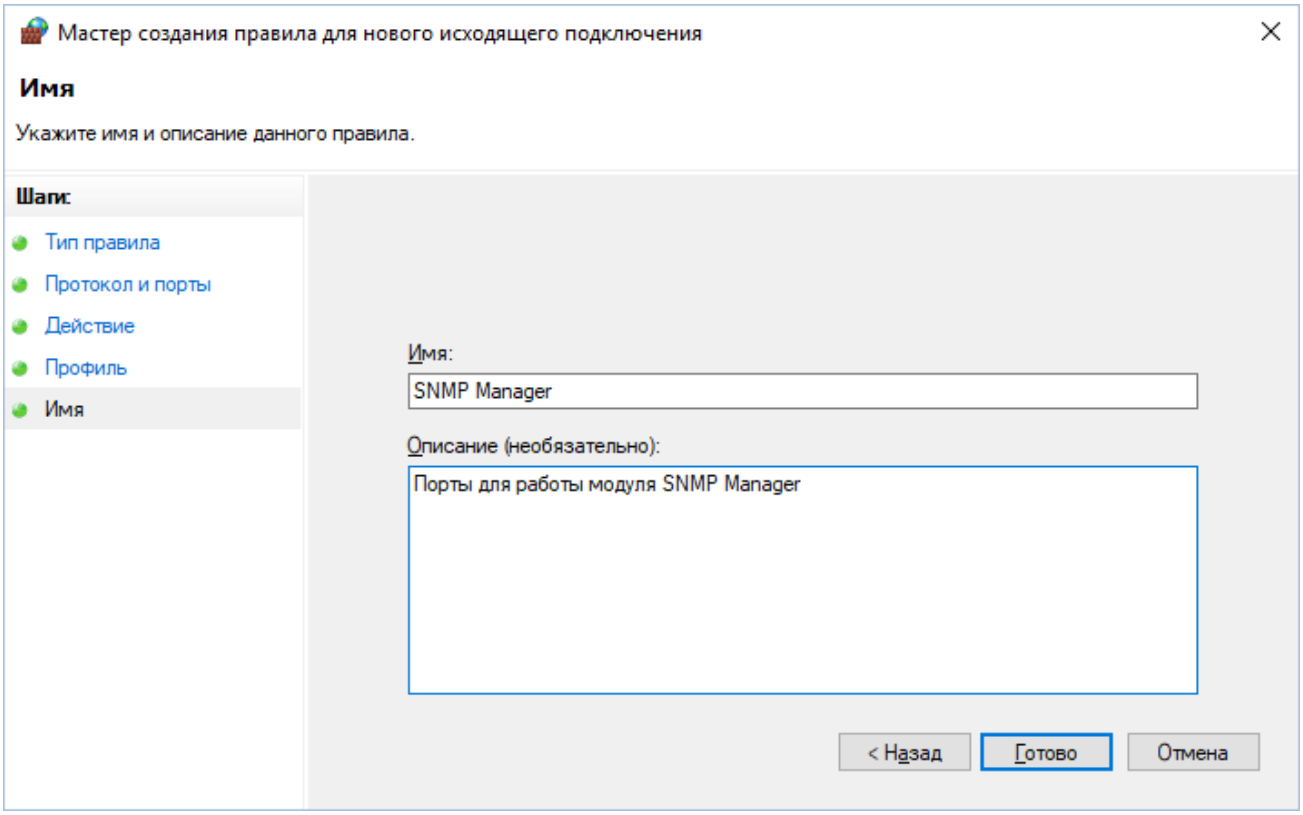
5. Выберите действие **Разрешить подключение** и нажмите кнопку **Далее**.



6. Укажите профили, к которым будет применяться правило, установив соответствующие флаги, и нажмите кнопку **Далее**.



7. Укажите для создаваемого правила имя, описание и нажмите кнопку **Готово**.



18.2. ОС Linux

ОБРАТИТЕ ВНИМАНИЕ

Настройку правил брандмауэра UFW следует выполнять только если данный брандмауэр установлен и используется в системе. Если в системе используется другой брандмауэр, то настройку правил следует выполнять в нём.

ПРИМЕЧАНИЕ

Чтобы установить брандмауэр UFW, выполните команду установки с помощью пакетного менеджера apt:

```
sudo apt install ufw
```

Чтобы настроить правила брандмауэра UFW:

1. Проверьте статус UFW командой:

```
sudo ufw status verbose
```

2. Если UFW отключен, то его необходимо включить. Для этого выполните команду:

```
sudo ufw enable
```

3. Запретите все входящие и исходящие подключения, если они не соответствуют правилам UFW, выполнив команды:

```
sudo ufw default deny incoming
```

```
sudo ufw default deny outgoing
```

4. Для настройки правил для входящих подключений выполните команду, с указанием порта и протокола, для которых требуется разрешить подключение:

```
sudo ufw allow in 4572/tcp
```

ОБРАТИТЕ ВНИМАНИЕ

Протоколы и порты, используемые компонентами Систэм Платформ для входящих подключений, приведены в разделе Порты для входящих подключений (см. стр. 125).

5. Для настройки правил для исходящих подключений выполните команду, с указанием порта и протокола, для которых требуется разрешить подключение:

```
sudo ufw allow out 161/upd
```

ОБРАТИТЕ ВНИМАНИЕ

Протоколы и порты, используемые компонентами Систэм Платформ для исходящих подключений, приведены в разделе Порты для исходящих подключений (см. стр. 126).

18.3. Порты для входящих подключений

Порты, через которые компоненты Систэм Платформ получают данные, приведены в таблице.

Компонент	Порт	Примечание
SePlatform.Data Server	TCP:4572	Подключение к SePlatform.Data Server приложений Статистика, Конфигуратор, Управляющий
	TCP:4388	Модуль TCP Server - подключение клиентов
	TCP:6551	Модуль резервирования - порт основного канала для подключения резервной пары
	TCP:6552	Модуль резервирования - порт резервного канала для подключения резервной пары
	TCP:6514	Модуль Syslog Server - получение данных по TLS
	UDP:514	Модуль Syslog Server - получение данных по UDP
	TCP:8080	Модуль OPC UA - получение данных по протоколу HTTP/HTTPS
	TCP:62544	Модуль OPC UA - получение данных по протоколу OPC.TCP
	TCP:2404	Модуль IEC Slave - подключение опросчика
	TCP:502	Модуль Modbus TCP Slave - подключение опросчика
SePlatform.AccessPoint	TCP:4976	Подключение к SePlatform.AccessPoint приложений Статистика, Конфигуратор
	TCP:4949	Получение исторических данных от SePlatform.Historian
SePlatform.Imitator	TCP:4983	Подключение к SePlatform.Imitator приложений Статистика, Конфигуратор
SePlatform.Historian	TCP:3388	Подключение приложения Статистика
	TCP:4949	Сохранение данных
SePlatform.Domain	TCP:1020	**SePlatform.Net.Agent**
	TCP:1010	**SePlatform.Domain.Agent**
SePlatform.Security	TCP:389	LDAP-сервер - запросы данных пользователей, их прав, конфигурирование
SePlatform.License Server	TCP:15150	Подключение для запроса лицензий
	TCP:15151	Подключение приложения Статистика

Компонент	Порт	Примечание
SePlatform.HMI.WebViewer	TCP:8080	Незащищенные соединения по веб-сокету
	TCP:4430	Безопасные соединения по веб-сокету
SePlatform.Mapping Server	TCP:5432	Доступ к данным через PostgreSQL

18.4. Порты для исходящих подключений

Порты, через которые компоненты Систэм Платформ отправляют данные, приведены в таблице.

Компонент	Порт	Примечание
SePlatform.Data Server	TCP:4572	Для приложений Статистика, Конфигуратор, Управляющий
	TCP:3388	Предоставление статистики в SePlatform.Historian
	TCP:4949	Сохранение данных в SePlatform.Historian
	TCP:4388	Модуль TCP Server - предоставление данных клиентам
	UDP:161	Модуль SNMP Manager - опрос агента
	UDP:162	Модуль SNMP Manager - trap-уведомления
	TCP:6551	Модуль резервирования - порт основного канала для подключения к резервной паре
	TCP:6552	Модуль резервирования - порт резервного канала для подключения к резервной паре
	TCP:102	Модуль IEC-61850 Client - опрос устройств
	UDP:9600	Модуль FINS Client - опрос устройств
	TCP:8080	Модуль OPC UA Client - порт HTTP/HTTPS протокола
	TCP:62544	Модуль OPC UA Client - порт OPC.TCP протокола
	TCP:2404	Модуль IEC-104 Master - опрос подчиненной станцией
	TCP:502	Модуль Modbus TCP Master -опрос подчиненной станцией
SePlatform.AccessPoint	TCP:4388	Подключение к SePlatform.Data Server
SePlatform.Imitator	TCP:4949	Подключение к SePlatform.Historian для чтения истории, записи имитационных данных
SePlatform.Domain	TCP:1020	**SePlatform.Net.Agent**
	TCP:1010	**SePlatform.Domain.Agent**
SePlatform.Security	TCP:389	Конфигуратор, Агент

Компонент	Порт	Примечание
SePlatform.Development Studio	TCP:1010	`SePlatform.Net.Agent`
SePlatform.HMI.Designer	TCP:4388	Оперативные данные SePlatform.Data Server
	TCP:4950	Исторические данные SePlatform.Historian
SePlatform.HMI.Viewer	TCP:4388	Оперативные данные SePlatform.Data Server
	TCP:4950	Исторические данные SePlatform.Historian
SePlatform.HMI.Alarms	TCP:4388	Оперативные данные SePlatform.Data Server
	TCP:4950	Исторические данные SePlatform.Historian
SePlatform.HMI.Trends	TCP:4388	Оперативные данные SePlatform.Data Server
	TCP:4950	Исторические данные SePlatform.Historian

19. Настройка DCOM

ОБРАТИТЕ ВНИМАНИЕ

Перед использованием компонентов Систэм Платформ в ОС Windows проверьте настройку DCOM.

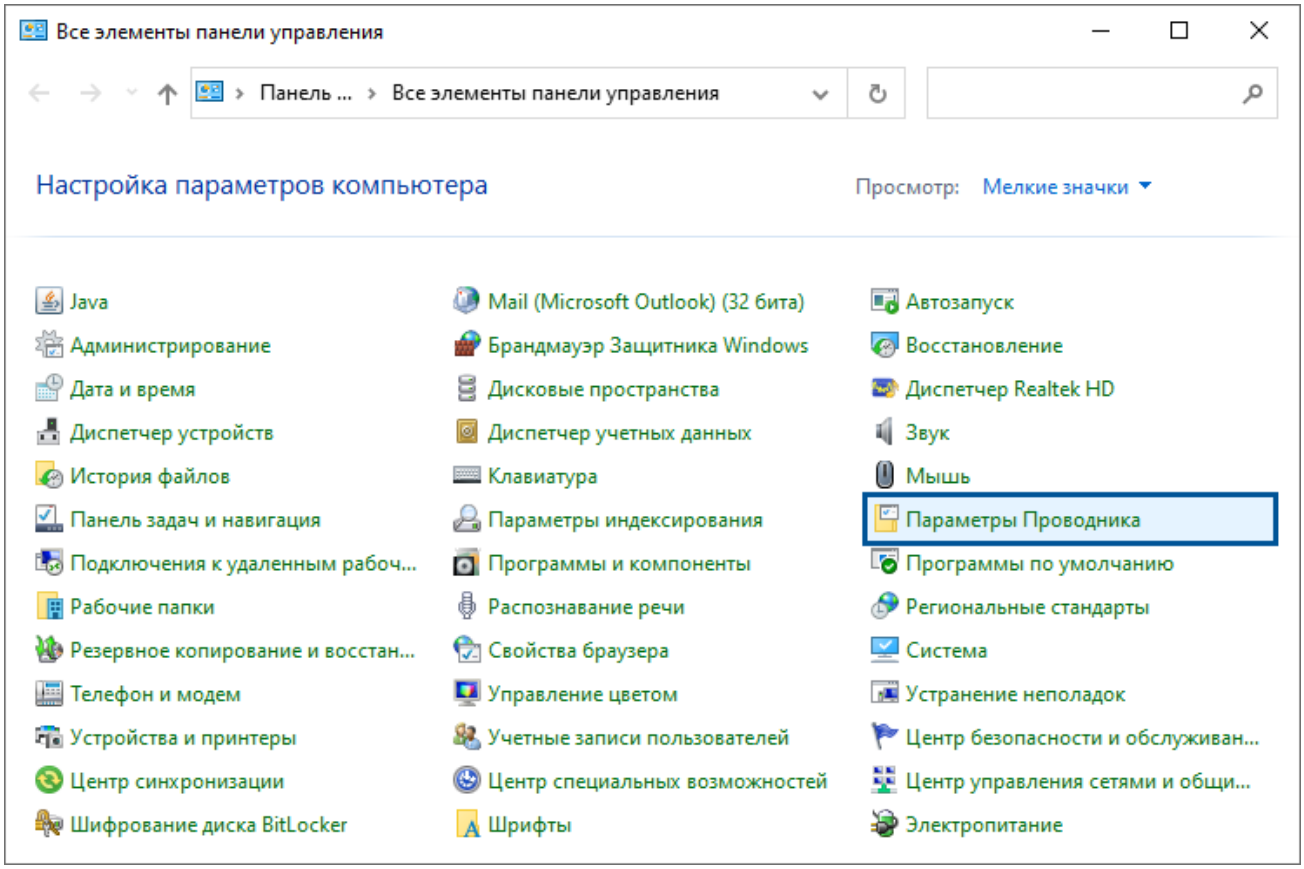
Для корректной работы компонентов Систэм Платформ, работающих по спецификациям OPC, настройте сетевые параметры и параметры безопасности DCOM. При отсутствии настройки DCOM возможно:

- отсутствие соединения и обмена данными по спецификации OPC DA между компонентами Систэм Платформ;
- отсутствие подключения к SePlatform.Historian;
- некорректное отображение режимов серверов резервной пары.

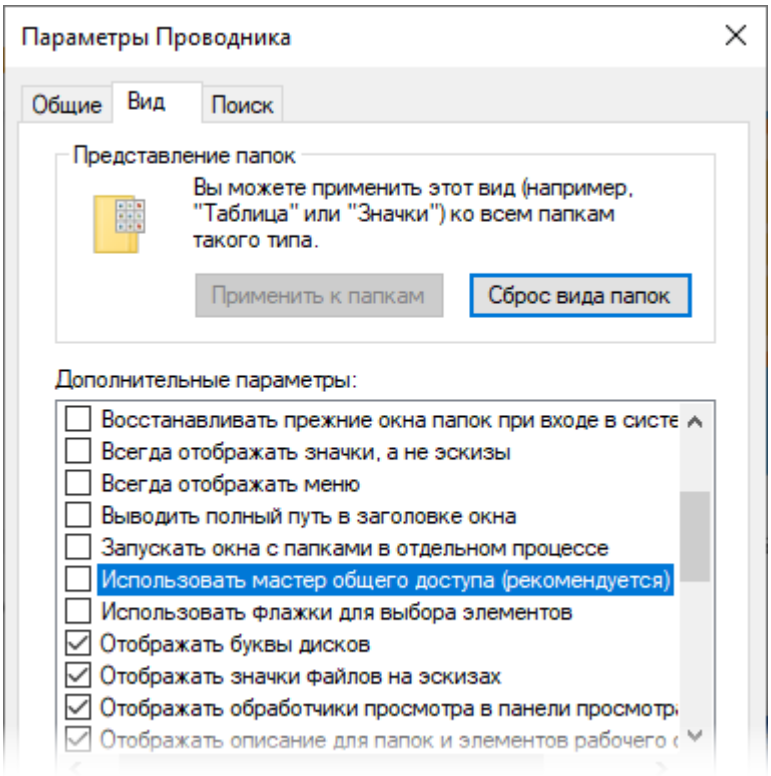
19.1. Настройка доступа

Чтобы все подключаемые пользователи идентифицировались на компьютере OPC-сервера под своими учетными записями, а не под учетной записью **«Гость»**:

1. Перейдите в меню `Пуск → Служебные – Windows → Панель управления → Все элементы панели управления → Параметры Проводника`.



2. В открывшемся окне **Параметры Проводника** на вкладке **Вид** снимите флаг **«Использовать мастер общего доступа»**.



19.2. Рекомендуемые настройки DCOM

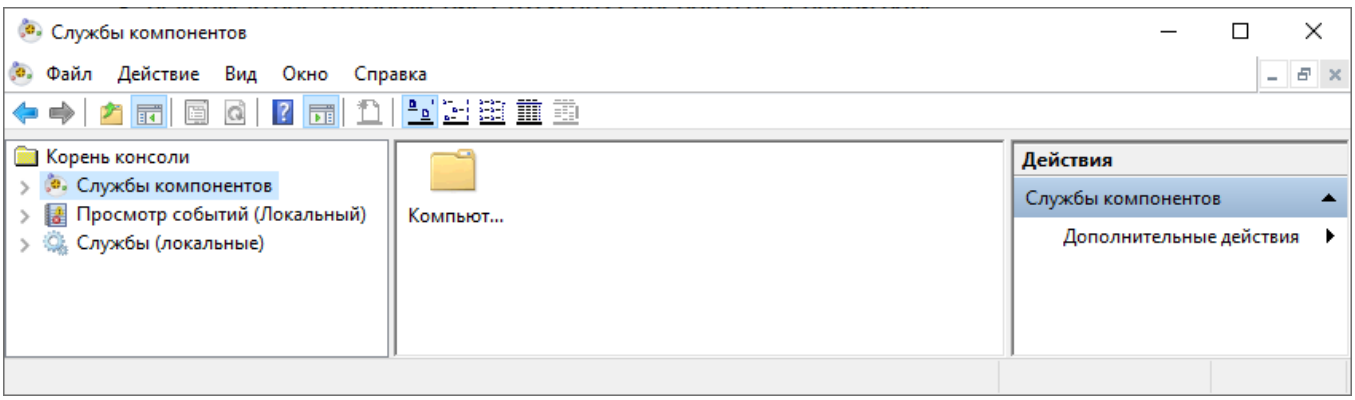
Для обеспечения работоспособности компонентов Систэм Платформ выполните рекомендуемые настройки безопасности DCOM.

Перед настройкой DCOM на компьютере:

1. Отключите брандмауэр.
2. Отключите мастер общего доступа.

Для настойки параметров DCOM используется системная программа ОС Windows Службы компонентов. Для запуска программы перейдите в меню `Пуск → Средства администрирования → Службы компонентов`, либо в поле поиска на панели задач или в окне **Выполнить** введите команду:

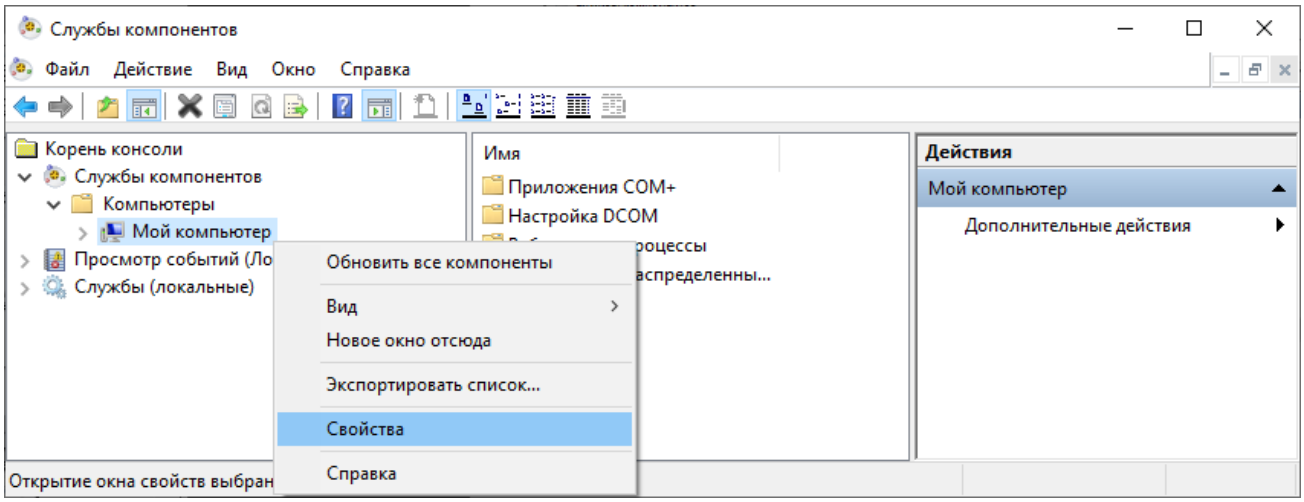
```
dcomcnfg
```



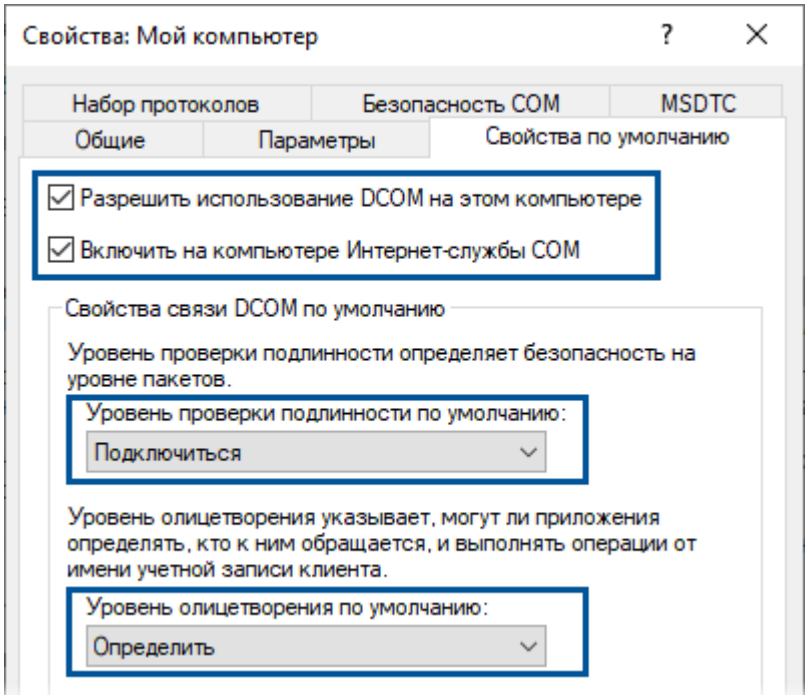
19.2.1. Настройка безопасности DCOM

Чтобы настроить параметры безопасности DCOM:

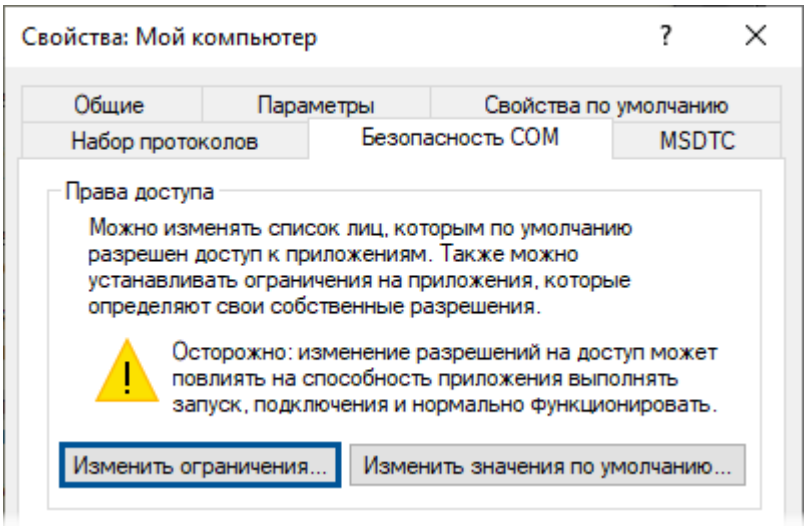
1. В окне Службы компонентов выберите узел `Корень консоли → Службы компонентов → Компьютеры → Мой компьютер`.
2. В контекстном меню узла `Мой компьютер` и выберите пункт **Свойства**.



3. В открывшемся окне **Свойства: Мой компьютер** перейдите на вкладку **Свойства по умолчанию**:
   - установите флаг **«Разрешить использование DCOM на этом компьютере»**;
   - установите флаг **«Включить на компьютере Интернет-службы COM»**;
   - параметру **Уровень проверки подлинности по умолчанию** установите значение **«Подключиться»**;
   - параметру **Уровень олицетворения по умолчанию** установите значение **«Определить»**.

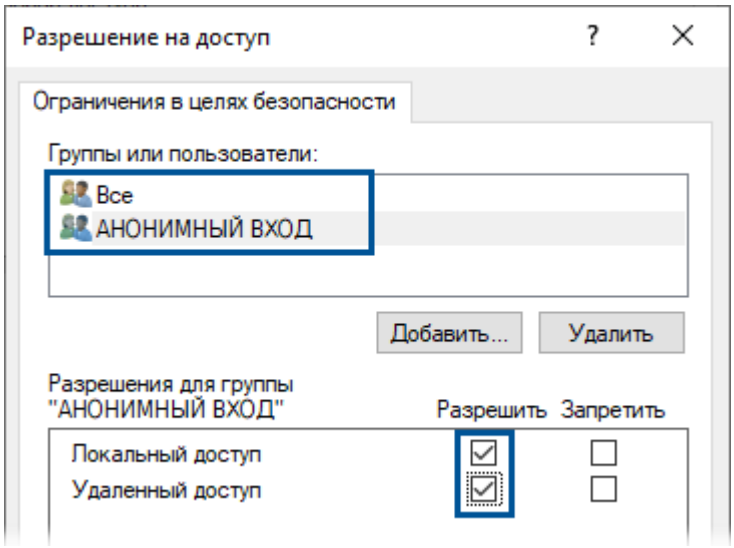


4. Перейдите на вкладку **Безопасность COM** и в группе **Права доступа** нажмите кнопку **Изменить ограничения...**.



5. В открывшемся окне **Разрешение на доступ**:

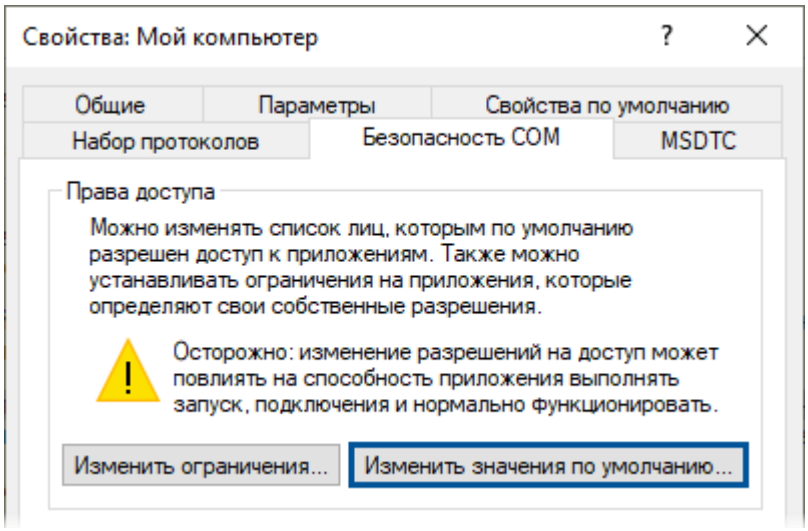
- Добавьте группы **«Все»** и **«АНОНИМНЫЙ ВХОД»**.
- Каждой группе установите флаги **«Разрешить»** для пунктов **Локальный доступ** и **Удаленный доступ**.



ОБРАТИТЕ ВНИМАНИЕ

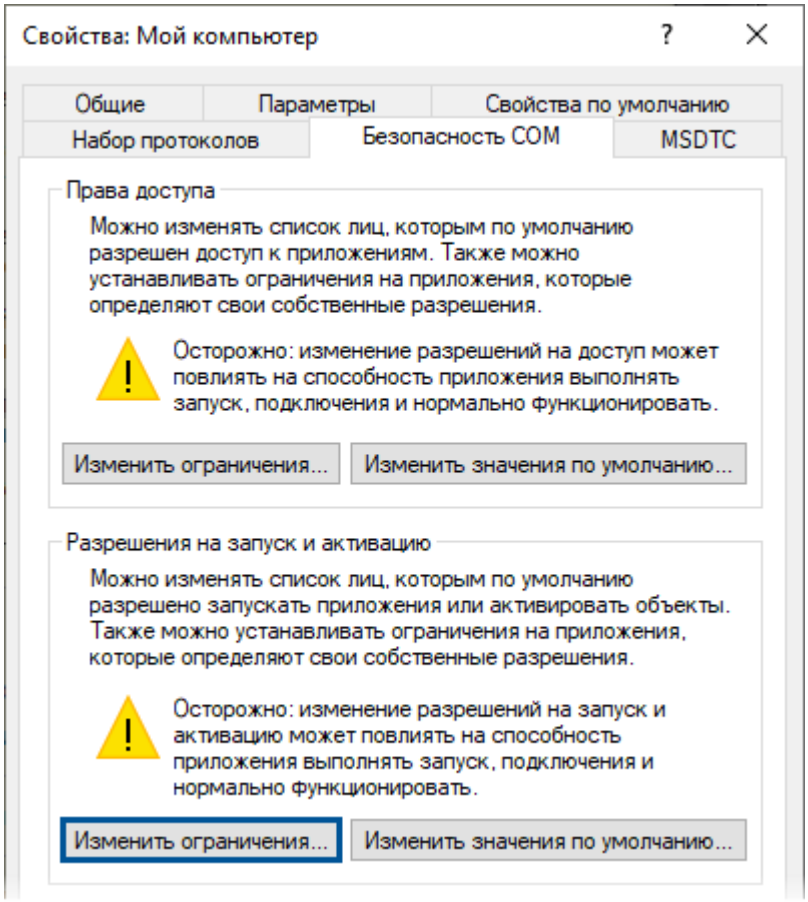
Разрешение доступа для групп **«Все»** и **«АНОНИМНЫЙ ВХОД»** предоставляет доступ к OPC-серверу большому количеству сторонних клиентов, но может снизить уровень безопасности компьютера.

6. В группе **Права доступа** нажмите кнопку **Изменить значения по умолчанию...**.

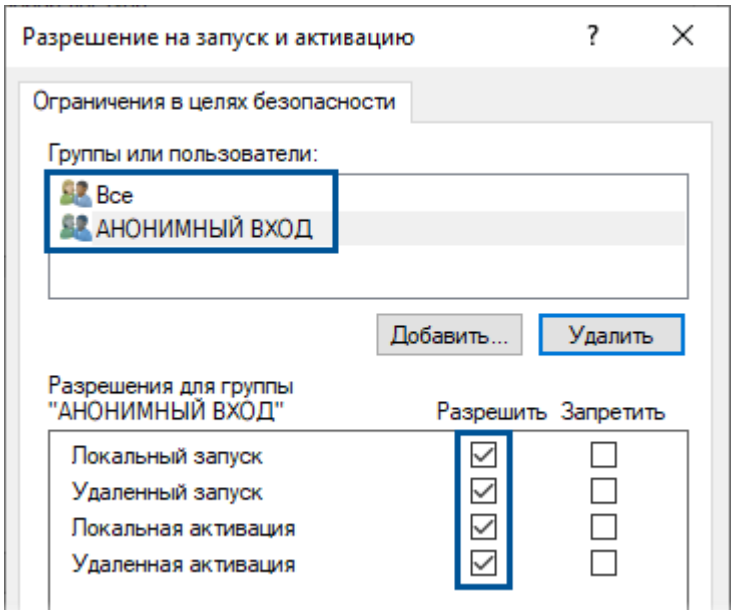


7. В открывшемся окне **Разрешение на доступ** выполните аналогичные настройки:
   - Добавьте группы **«Все»** и **«АНОНИМНЫЙ ВХОД»**.
   - Каждой группе установите флаги **«Разрешить»** для пунктов **Локальный доступ** и **Удаленный доступ**.

8. В окне **Свойства: Мой компьютер** на вкладке **Безопасность COM** в группе **Разрешения на запуск и активацию** нажмите кнопку **Изменить ограничения...**.



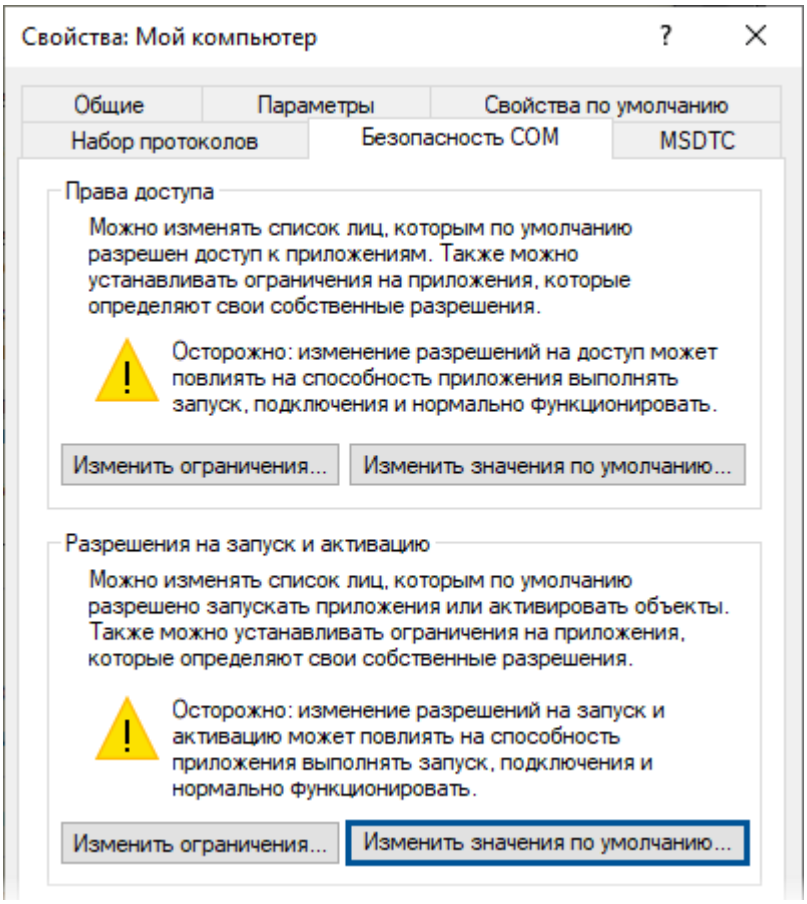
9. В открывшемся окне **Разрешение на запуск и активацию**:
   - Добавьте группы **«Все»** и **«АНОНИМНЫЙ ВХОД»**.
   - Каждой группе установите флаги **«Разрешить»** для всех вариантов запуска и активации.



ОБРАТИТЕ ВНИМАНИЕ

Разрешение доступа для групп **«Все»** и **«АНОНИМНЫЙ ВХОД»** предоставляет доступ к OPC-серверу большому количеству сторонних клиентов, но может снизить уровень безопасности компьютера.

10. В группе **Разрешения на запуск и активацию** нажмите кнопку **Изменить значения по умолчанию...**.



11. В открывшемся окне **Разрешение на запуск и активацию** выполните аналогичные настройки:
    - Добавьте группы **«Все»** и **«АНОНИМНЫЙ ВХОД»**.
    - Каждой группе установите флаги **«Разрешить»** для всех вариантов запуска и активации.

ОБРАТИТЕ ВНИМАНИЕ

Для применения настроек безопасности DCOM перезагрузите ОС Windows.

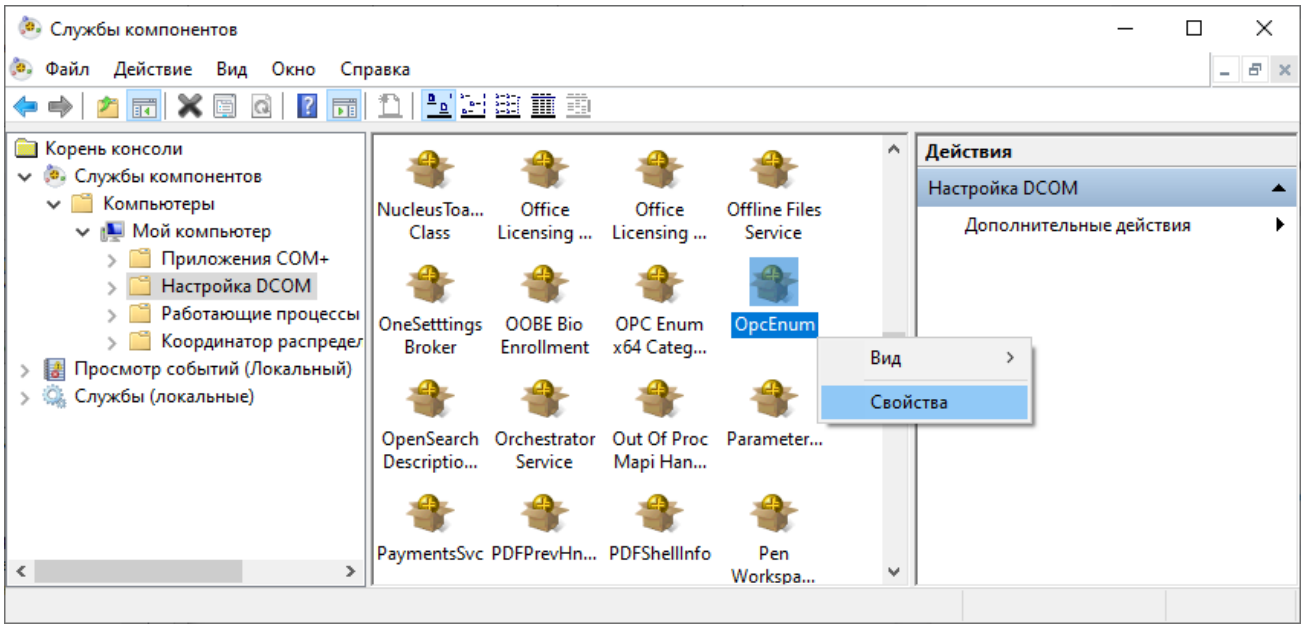
19.2.2. Настройка безопасности DCOM объектов

Выполните настройку безопасности DCOM для следующих приложений:

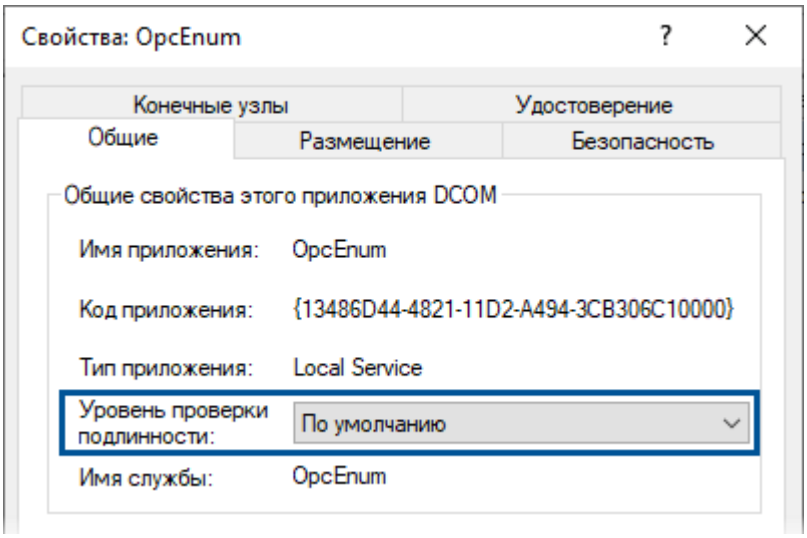
- OpcEnum - OPC-утилита, которая используется для доступа к данным удаленного OPC-сервера, формирует список доступных OPC-серверов;
- SePlatform.HDAServer - сервер OPC HDA;
- SePlatform.OPCDAServer - сервер OPC DA;
- SePlatform.OPCAEServer - сервер OPC AE;
- DCOM объект SePlatform.Historian.Server;
- дополнительные копии SePlatform.HDAServer, SePlatform.OPCDAServer, SePlatform.OPCAEServer.

Чтобы настроить параметры безопасности DCOM указанных объектов:

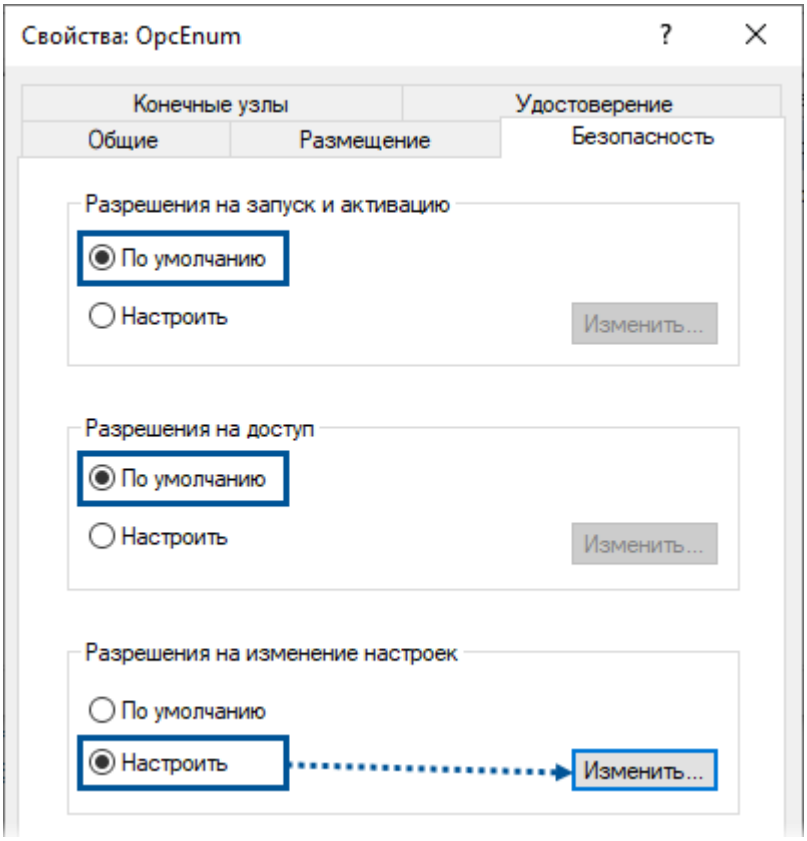
1. В окне Службы компонентов выберите узел `Корень консоли → Службы компонентов → Компьютеры → Мой компьютер → Настройка DCOM`.
2. В контекстном меню объекта выберите пункт **Свойства**.



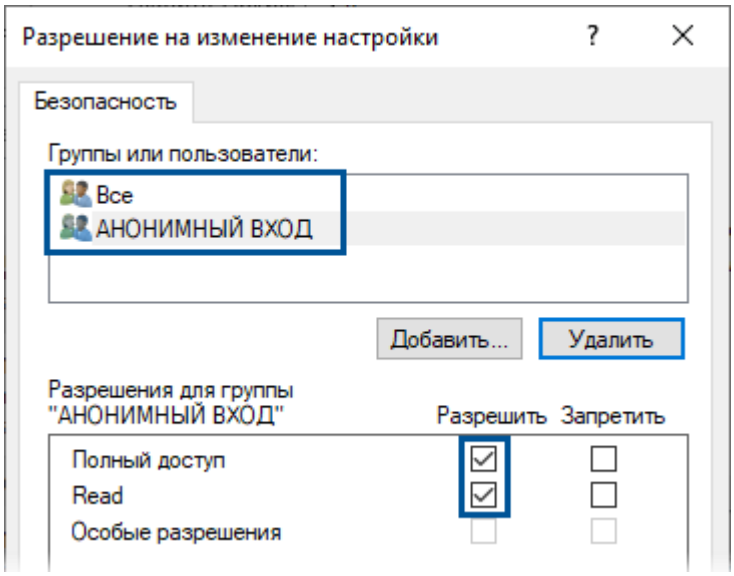
3. В открывшемся окне **Свойства** на вкладке **Общие** параметру **Уровень проверки подлинности** установите значение **«По умолчанию»**.



4. На вкладке **Безопасность** в группах **Разрешения на запуск и активацию** и **Разрешение на доступ** установите переключатель **«По умолчанию»**. В группе **Разрешения на изменение настроек** установите переключатель **«Настроить»** и нажмите кнопку **Изменить...**.



5. В открывшемся окне **Разрешение на изменение настройки**:
   - Добавьте группы **«Все»** и **«АНОНИМНЫЙ ВХОД»**.
   - Каждой группе установите флаги **«Разрешить»** для пунктов **Полный доступ** и **Read**.



19.3. Минимальные настройки DCOM

В случаях, когда требованиями безопасности запрещен доступ для групп **«Все»** и **«АНОНИМНЫЙ ВХОД»**, для обеспечения работоспособности компонентов Систэм Платформ выполните минимальные настройки безопасности DCOM.

Перед настройкой DCOM на компьютере:

1. Отключите брандмауэр.
2. Отключите мастер общего доступа.
3. Как для локального компьютера, так и для компьютера, состоящего в домене, определите пользователя или группу пользователей, которым будет предоставлен доступ к DCOM объектам.

Для более гибкого управления доступом в настройках безопасности используйте:

- созданную группу пользователей (далее группа **«Users»**);
- встроенную группу **«Пользователи DCOM»**.

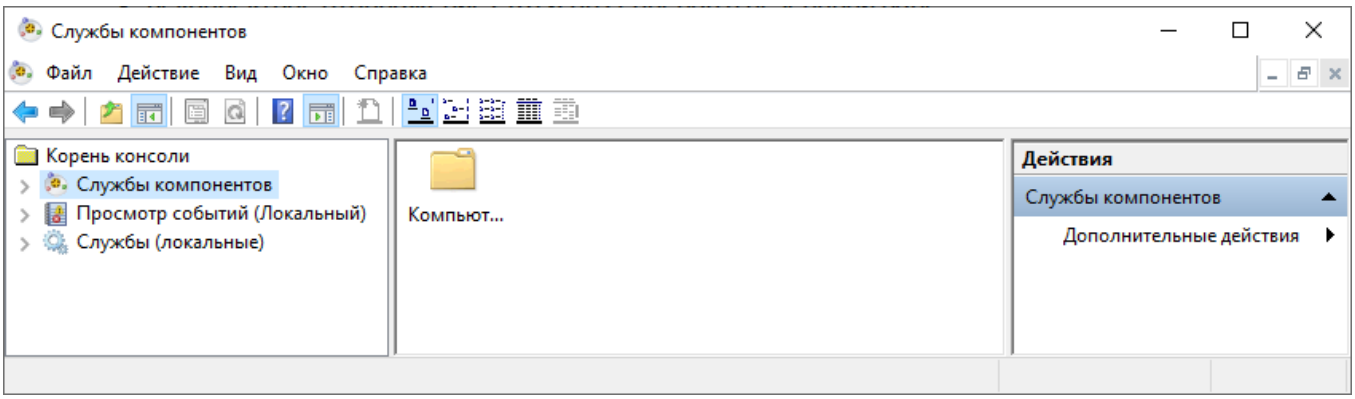
После создания группы добавьте в неё пользователей.

У пользователей, которым требуется доступ к настраиваемому компьютеру по DCOM, должно быть разрешение на доступ к DCOM на этом компьютере.

На серверном компьютере добавьте пользователя в группу, которой выданы разрешения в DCOM. Если серверный компьютер находится не в домене, то создайте локального пользователя с тем же именем и паролем, что на клиентском компьютере, и добавьте в группу, которой выданы разрешения в DCOM.

Для настойки параметров DCOM используется системная программа ОС Windows Службы компонентов. Для запуска программы перейдите в меню `Пуск → Средства администрирования → Службы компонентов`, либо в поле поиска на панели задач или в окне **Выполнить** введите команду:

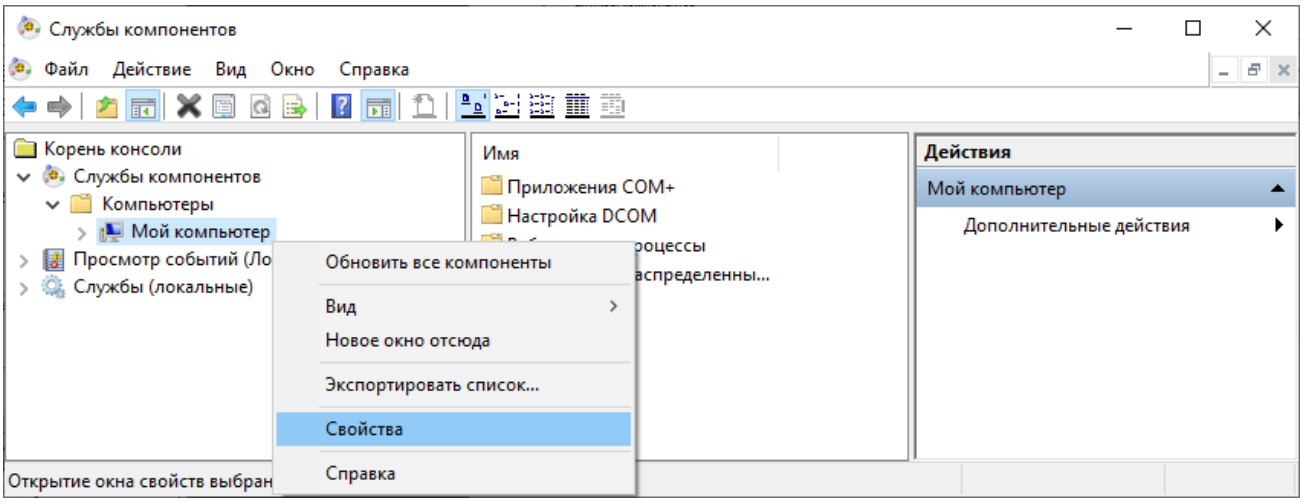
```
dcomcnfg
```



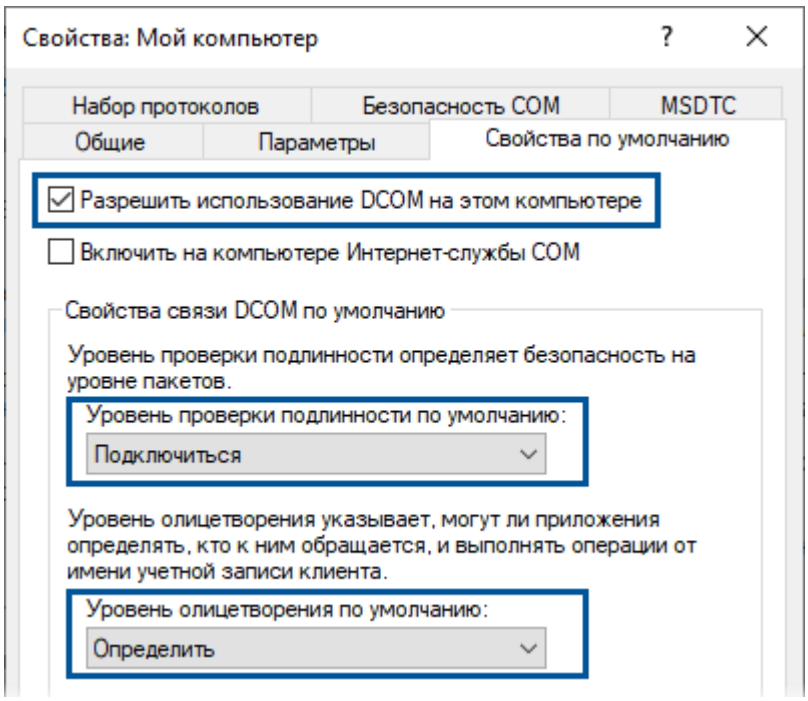
19.3.1. Настройка безопасности DCOM

Чтобы настроить параметры безопасности DCOM:

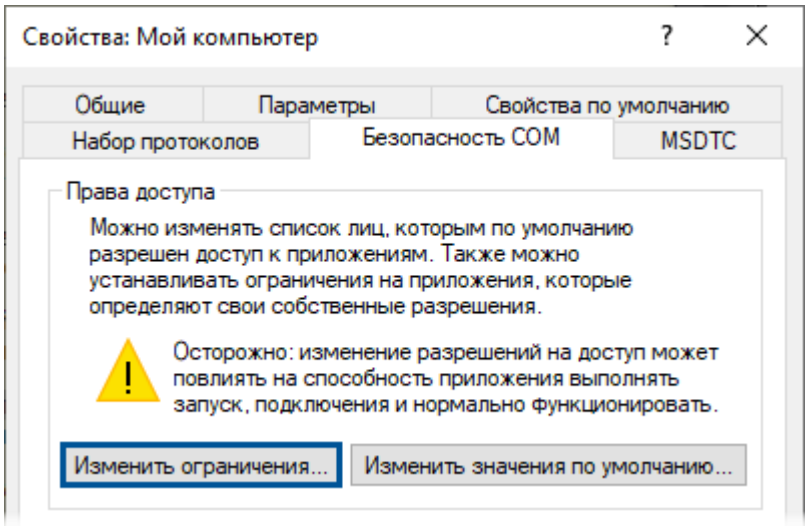
1. В окне Службы компонентов выберите узел `Корень консоли → Службы компонентов → Компьютеры → Мой компьютер`.
2. В контекстном меню узла `Мой компьютер` и выберите пункт **Свойства**.



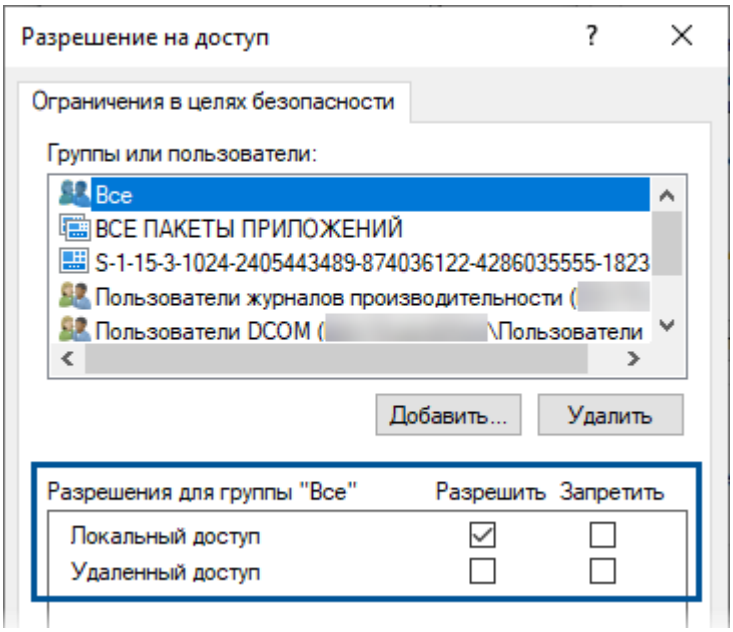
3. В открывшемся окне **Свойства: Мой компьютер** перейдите на вкладку **Свойства по умолчанию**:
   - установите флаг **«Разрешить использование DCOM на этом компьютере»**;
   - параметру **Уровень проверки подлинности по умолчанию** установите значение **«Подключиться»**;
   - параметру **Уровень олицетворения по умолчанию** установите значение **«Определить»**.



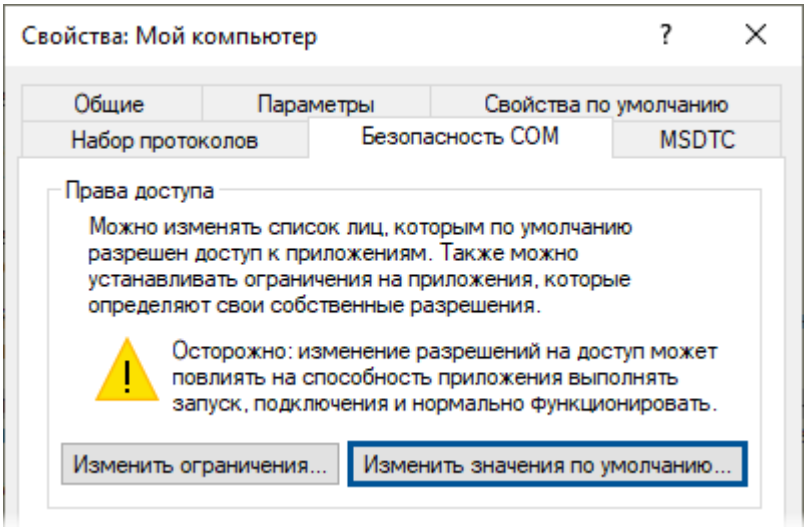
4. Перейдите на вкладку **Безопасность COM** и в группе **Права доступа** нажмите кнопку **Изменить ограничения...**.



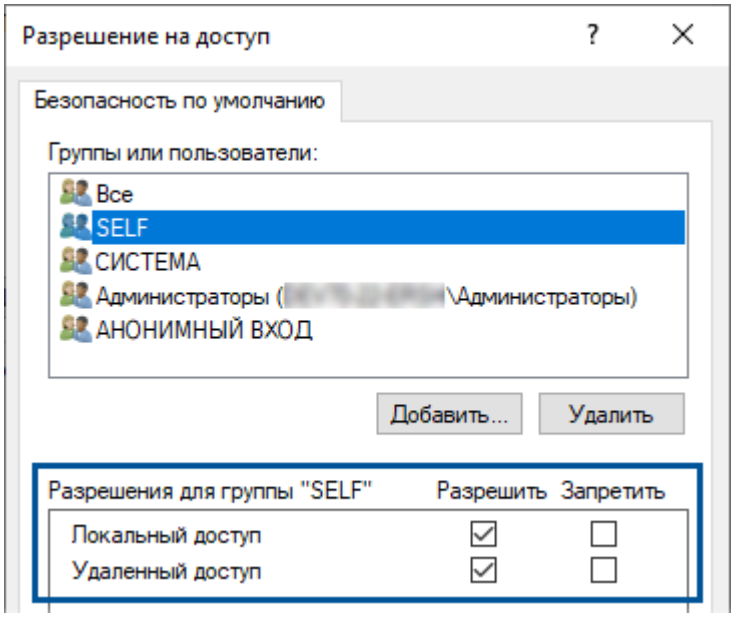
5. В открывшемся окне **Разрешение на доступ** группам установите флаги **«Разрешить»** или **«Запретить»**:
   - для группы **«Users»** разрешите локальный и удаленный доступ;
   - для группы **«Все»** разрешите только локальный доступ;
   - для группы **«Пользователи журналов производительности»** разрешите локальный и удаленный доступ;
   - для группы **«Пользователи DCOM»** разрешить локальный и удаленный доступ.



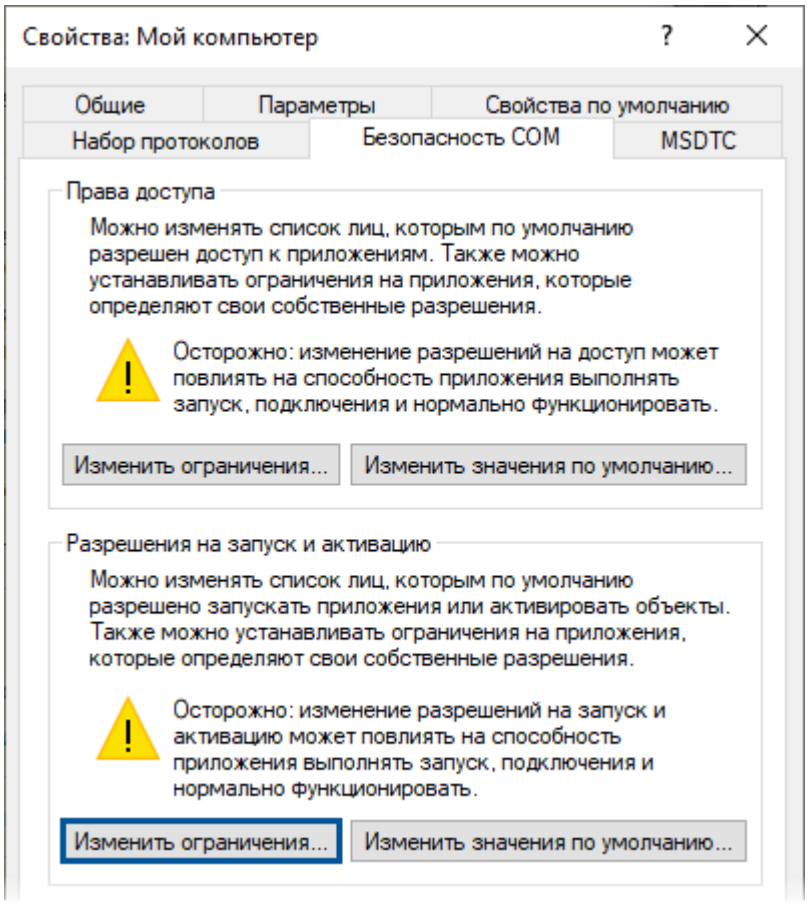
6. В группе **Права доступа** нажмите кнопку **Изменить значения по умолчанию...**.



7. В открывшемся окне **Разрешение на доступ** группам установите флаги **«Разрешить»** или **«Запретить»**:
   - для группы **«SELF»** разрешите локальный и удаленный доступ;
   - для группы **«СИСТЕМА»** разрешите только локальный доступ;
   - для группы **«Администраторы»** разрешите локальный и удаленный доступ.

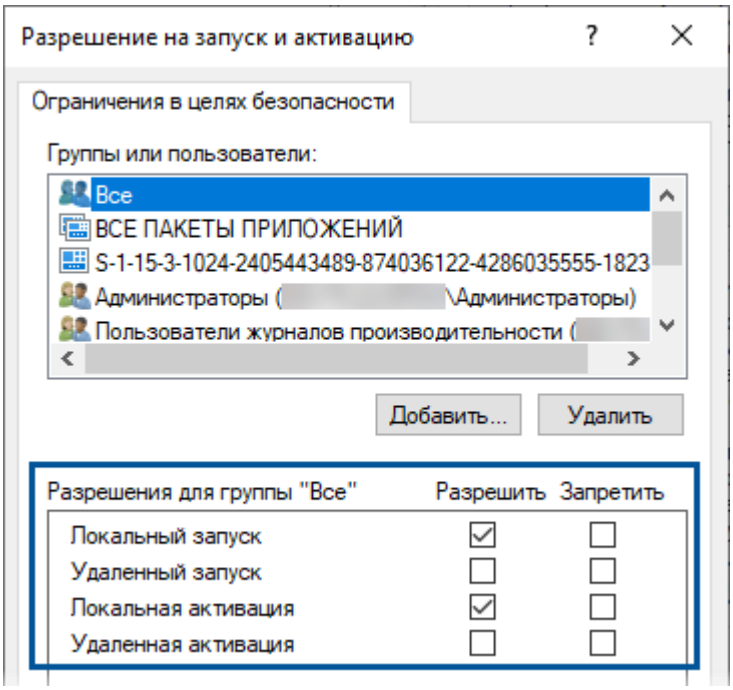


8. В окне **Свойства: Мой компьютер** на вкладке **Безопасность COM** в группе **Разрешения на запуск и активацию** нажмите кнопку **Изменить ограничения...**.

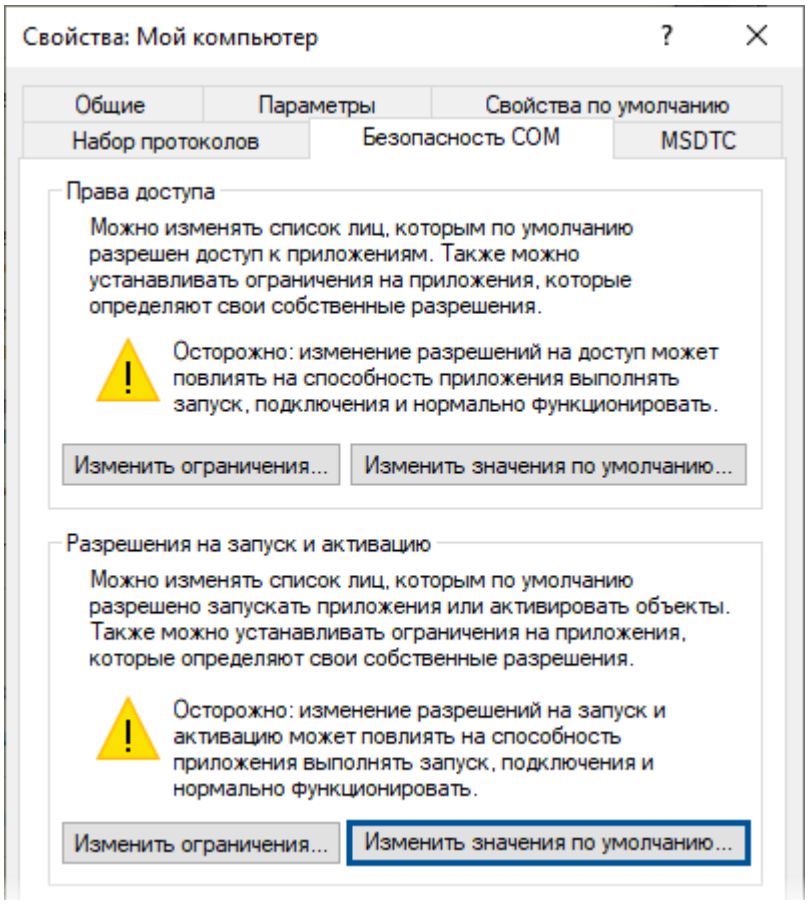


9. В открывшемся окне **Разрешение на запуск и активацию** группам установите флаги **«Разрешить»** или **«Запретить»**:

- для группы **«Users»** разрешите локальный и удаленный запуск, локальную и удаленную активацию;
- для группы **«Все»** разрешите только локальный запуск и активацию;
- для группы **«Пользователи журналов производительности»** разрешите локальный и удаленный запуск, локальную и удаленную активацию;
- для группы **«Пользователи DCOM»** разрешите локальный и удаленный запуск, локальную и удаленную активацию;
- для группы **«Администраторы»** разрешите локальный и удаленный запуск, локальную и удаленную активацию.

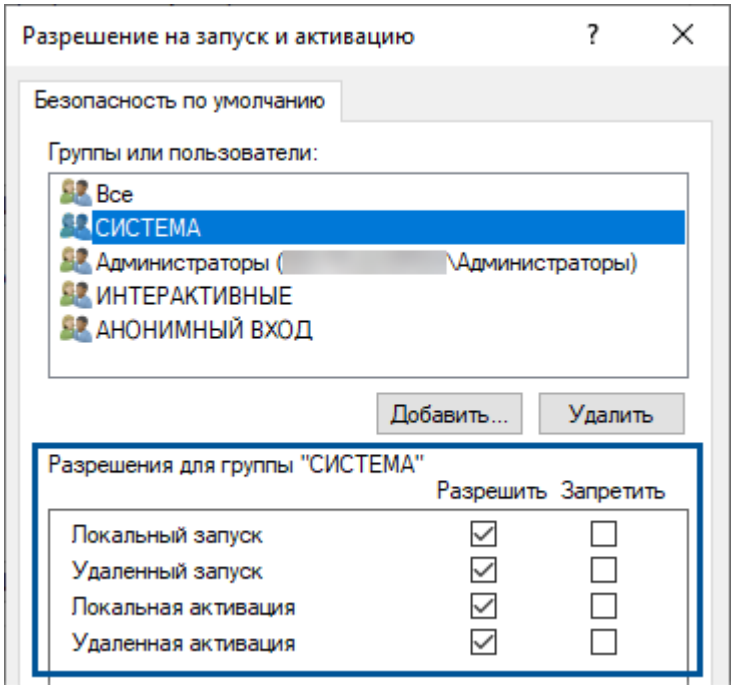


10. В группе **Разрешения на запуск и активацию** нажмите кнопку **Изменить значения по умолчанию...**.



11. В открывшемся окне **Разрешение на запуск и активацию** группам установите флаги **«Разрешить»** или **«Запретить»**:

- для группы **«СИСТЕМА»** разрешите локальный и удаленный запуск, локальную и удаленную активацию;
- для группы **«Администраторы»** разрешите локальный и удаленный запуск, локальную и удаленную активацию;
- для группы **«ИНТЕРАКТИВНЫЕ»** разрешите локальный и удаленный запуск, локальную и удаленную активацию.



ОБРАТИТЕ ВНИМАНИЕ

Группа **«Все»** неявно включает в себя учетную запись **«СИСТЕМА»** и не включает учетную запись **«АНОНИМНЫЙ ВХОД»**.

Если использование группы **«Все»** не соответствует требованиям безопасности, то для сохранения работоспособности ОС обязательно явно пропишите права доступа и разрешения на запуск и активацию для групп:

- **«СИСТЕМА»**;
- **«LOCAL SERVICE»**;
- **«NETWORK SERVICE»**;
- **«Администраторы»** (локальные);
- **«Пользователи»** (локальные).

Для указанных выше групп настройте только ограничения, не изменяя значения по умолчанию:

1. Откройте окно Службы компонентов и выберите узел `Корень консоли → Службы компонентов → Компьютеры → Мой компьютер`.
2. В контекстном меню узла `Мой компьютер` и выберите пункт **Свойства**.
3. В открывшемся окне **Свойства: Мой компьютер** перейдите на вкладку **Безопасность COM**.
4. В группе **Права доступа** нажмите кнопку **Изменить ограничения...**.

5. В открывшемся окне **Разрешение на доступ**:
   - для группы **«Users»** разрешите локальный и удаленный доступ;
   - для группы **«СИСТЕМА»** разрешите только локальный доступ;
   - для группы **«LOCAL SERVICE»** разрешите только локальный доступ;
   - для группы **«NETWORK SERVICE»** разрешите только локальный доступ;
   - для группы **«Администраторы»** разрешите локальный и удаленный доступ;
   - для группы **«Пользователи»** разрешите только локальный доступ.
6. В группе **Разрешения на запуск и активацию** нажмите кнопку **Изменить ограничения...**.
7. В открывшемся окне **Разрешение на запуск и активацию** выполните:
   - для группы **«Users»** разрешите локальный и удаленный запуск, локальную и удаленную активацию;
   - для группы **«СИСТЕМА»** разрешите только локальный запуск и активацию;
   - для группы **«LOCAL SERVICE»** разрешите только локальный запуск и активацию;
   - для группы **«NETWORK SERVICE»** разрешите только локальный запуск и активацию;
   - для группы **«Администраторы»** разрешите локальный и удаленный запуск, локальную и удаленную активацию;
   - для группы **«Пользователи»** разрешите только локальный запуск и активацию.

19.3.2. Настройка безопасности DCOM объектов

Выполните настройку безопасности DCOM для следующих серверных приложений:

- OpcEnum - OPC-утилита, которая используется для доступа к данным удаленного OPC-сервера, формирует список доступных OPC-серверов;
- SePlatform.HDAServer - сервер OPC HDA;
- SePlatform.OPCDAServer - сервер OPC DA;
- SePlatform.OPCAEServer - сервер OPC AE;
- DCOM объект SePlatform.Historian.Server;
- дополнительные копии SePlatform.HDAServer, SePlatform.OPCDAServer, SePlatform.OPCAEServer.

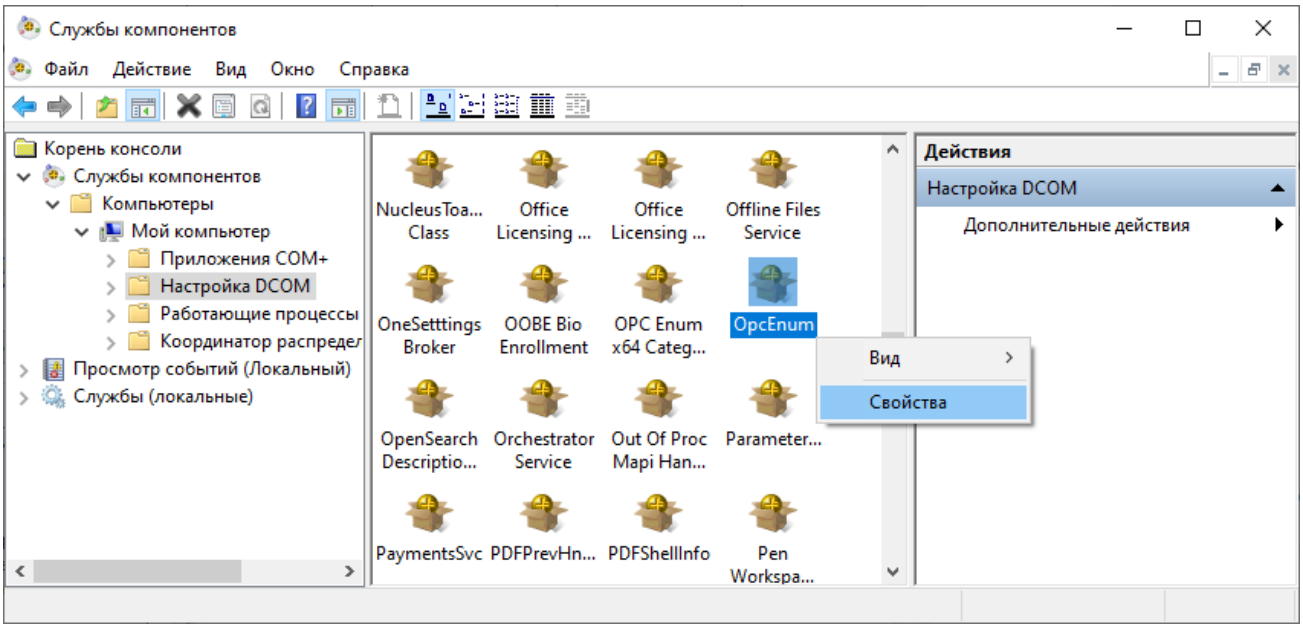
ОБРАТИТЕ ВНИМАНИЕ

Если у группы **«Users»** нет разрешений в глобальной безопасности DCOM для ОС, то её разрешения в конкретном DCOM объекте игнорируются ОС.

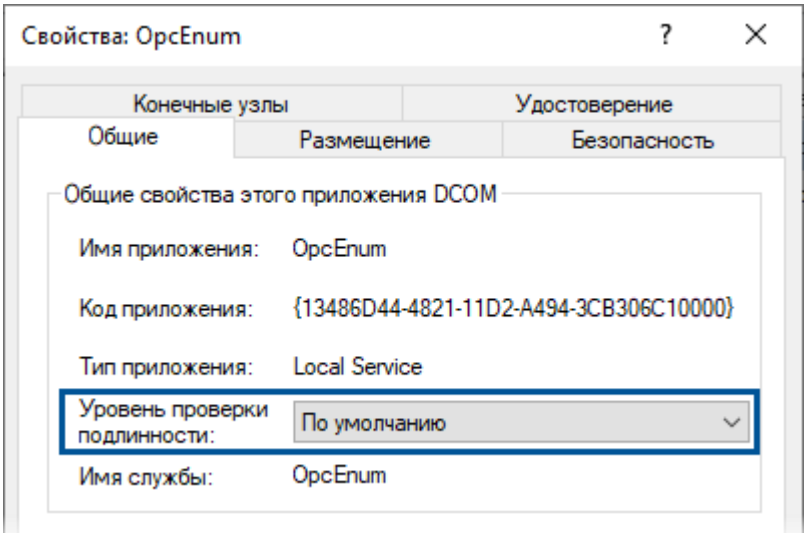
Чтобы настроить безопасность DCOM указанных приложений:

1. В окне Службы компонентов выберите узел `Корень консоли → Службы компонентов → Компьютеры → Мой компьютер → Настройка DCOM`.

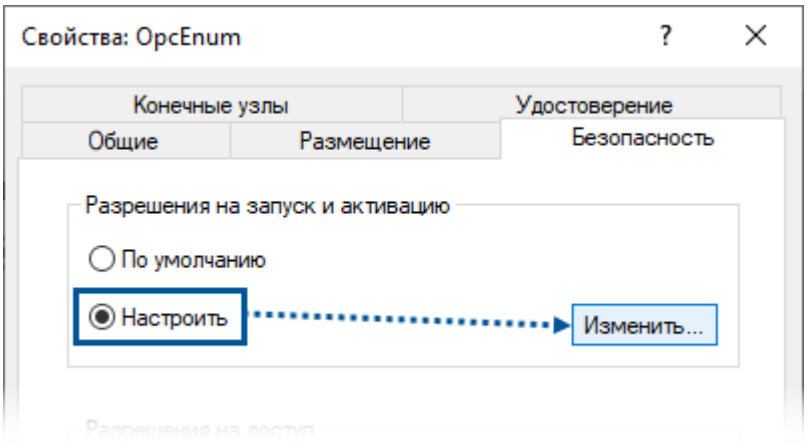
2. В контекстном меню объекта выберите пункт **Свойства**.



3. В открывшемся окне **Свойства** на вкладке **Общие** параметру **Уровень проверки подлинности** установите значение **«По умолчанию»**.



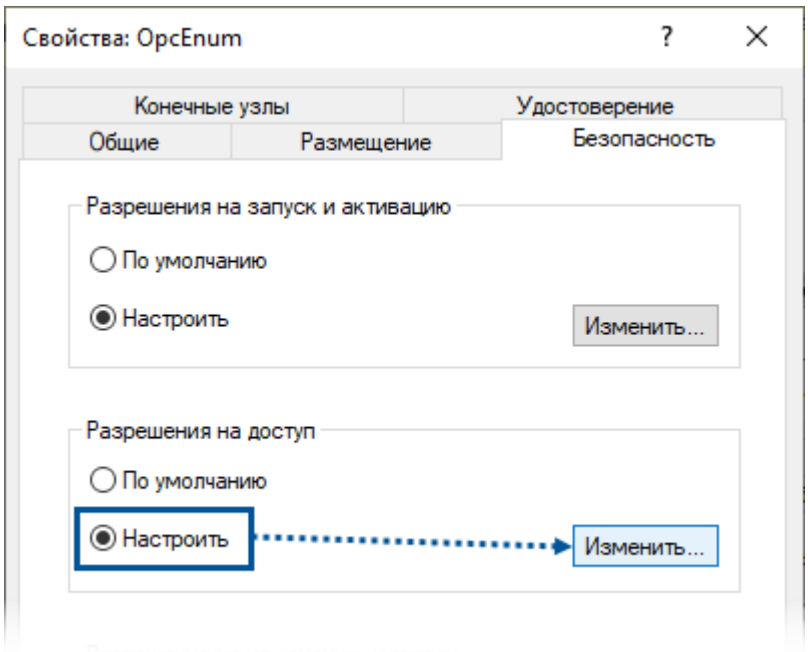
4. На вкладке **Безопасность** в группе **Разрешения на запуск и активацию** установите переключатель **«Настроить»** и нажмите кнопку **Изменить...**.



5. В открывшемся окне **Разрешения на запуск и активацию**:

   - для группы **«Users»** разрешите локальный и удаленный запуск, локальную и удаленную активацию;
   - для группы **«СИСТЕМА»** разрешите локальный и удаленный запуск, локальную и удаленную активацию;
   - для группы **«Администраторы»** разрешите локальный и удаленный запуск, локальную и удаленную активацию.

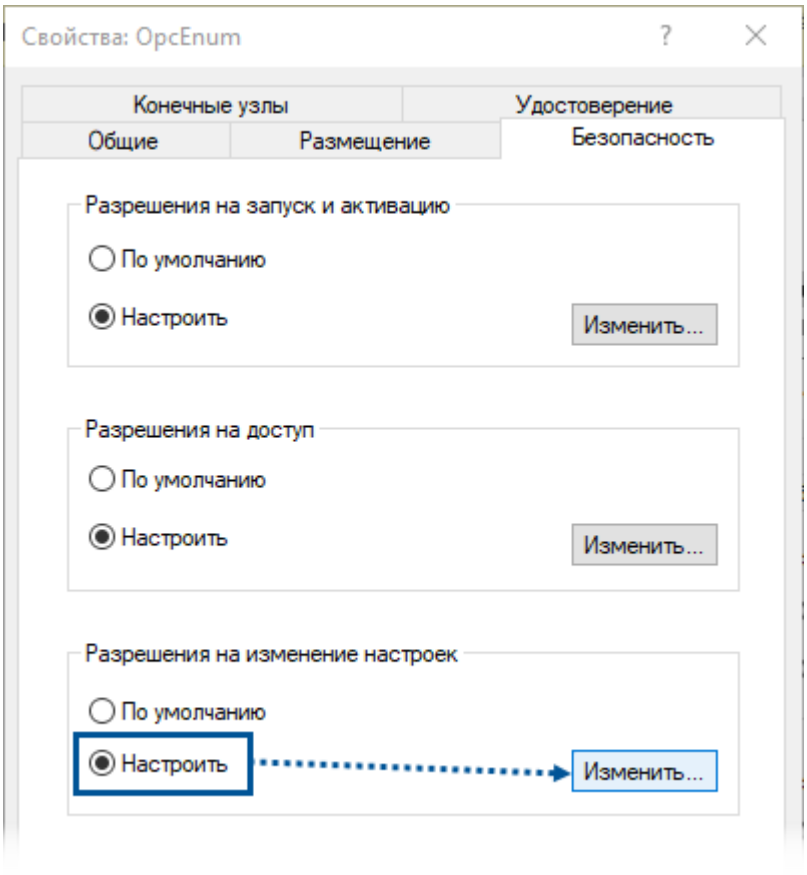
6. В группе **Разрешения на доступ** установите переключатель **«Настроить»** и нажмите кнопку **Изменить...**.



7. В открывшемся окне **Разрешение на доступ**:

   - для группы **«Users»** разрешите локальный и удаленный доступ;
   - для группы **«СИСТЕМА»** разрешите только локальный доступ;
   - для группы **«Администраторы»** разрешите локальный и удаленный доступ.

8. В группе **Разрешения на изменение настроек** установите переключатель **«Настроить»** и нажмите кнопку **Изменить...**.



9. В открывшемся окне **Разрешение на изменение настройки**:
   - для группы **«Users»** разрешите полный доступ;
   - для группы **«СИСТЕМА»** разрешите полный доступ;
   - для группы **«Администраторы»** разрешите полный доступ.

ОБРАТИТЕ ВНИМАНИЕ

После переустановки SePlatform.Data Server или перерегистрации его службы сбрасываются настройки COM серверов: SePlatform.OPCDAServer, SePlatform.HDAServer и SePlatform.OPCAEServer.

ПРИМЕЧАНИЕ

Для запрета автоматического запуска привязанной к DCOM объекту службы, в этом объекте запретите локальный и удаленный запуск (но активация должна быть разрешена) для всех без исключения учетных записей. Данное правило не распространяется на объект Opcenum. Для объекта Opcenum необходимо разрешить как локальный и удаленный запуск, так и локальную и удаленную активацию.

19.3.3. Запуск службы DCOM объекта от имени пользователя

В обычном случае, при работе запрос (клиент) - ответ (сервер), по отношению к настройкам безопасности DCOM - неважно от какого пользователя будет запущена служба (процесс), к которой относится DCOM объект. Клиенту необходимо лишь указать данные учетной записи с разрешенным доступом к DCOM объекту.

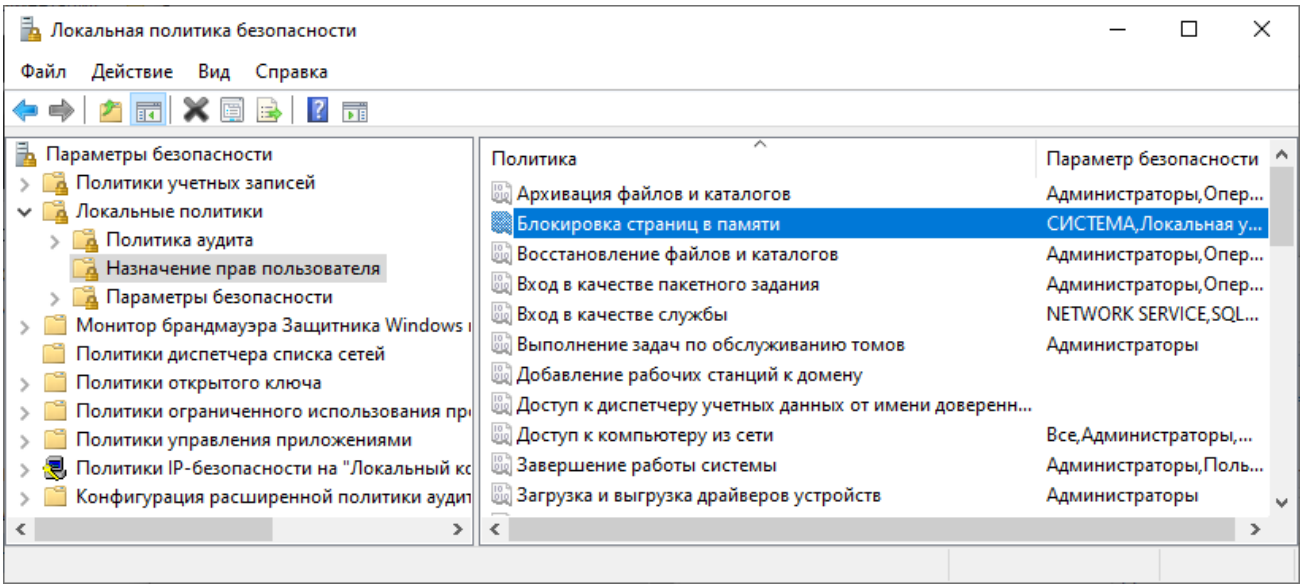
В случае callback функций (например подписка группы через интерфейс IOPCDataCallback) DCOM производит смену ролей, когда сервер становится клиентом, а клиент - сервером. Таким образом, сервер произведет попытку подключения к клиенту, используя данные учетной записи, под которой он был запущен. Поэтому, для успешного подключения сервера, клиенту необходимо знать эту учетную запись, либо локально, либо из домена.
Особенности использования автозапуска через DCOM:

- При использовании системной учетной записи в настройках удостоверения DCOM объекта для запуска будет использоваться учетная запись, указанная в параметрах входа службы.
- При указании учетной записи пользователя в настройках удостоверения DCOM объекта для запуска, эта же учетная запись будет записана в параметрах входа службы.
- Изменение учетной записи в параметрах входа службы не распространяется на учетную запись в настройках удостоверения DCOM объекта для запуска. Поэтому при автозапуске через DCOM служба будет запущена от учетной записи, указанной в параметрах входа, несмотря на настройки удостоверения в DCOM объекте.

При запуске службы **`SePlatform.Server`** от имени пользователя без прав администратора:

1. В файловой системе задайте:
   - права доступа пользователя к каталогу `C:\Program Files\SePlatform\SePlatform.Server`:
     - полный доступ;
     - изменение;
     - чтение и выполнение;
     - список содержимого папки;
     - чтение;
     - запись.
   - права доступа пользователя к каталогам с файловыми очередями модулей OPC AE Server, History Module (пути указаны в настройках модуля):
     - изменение;
     - чтение и выполнение;
     - список содержимого папки;
     - чтение;
     - запись.

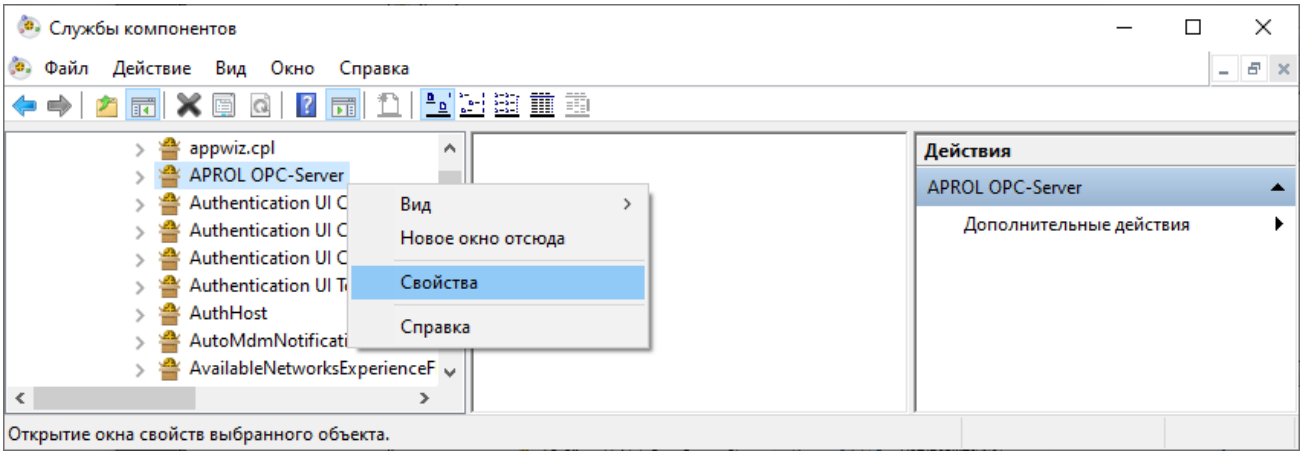
2. В настройках Локальной политики безопасности (`Пуск → Служебные → Панель управления → Администрирование → Локальная политика безопасности`) выберите узел `Параметры безопасности → Локальные политики → Назначение прав пользователя` и разрешите блокировку страниц памяти для пользователя.



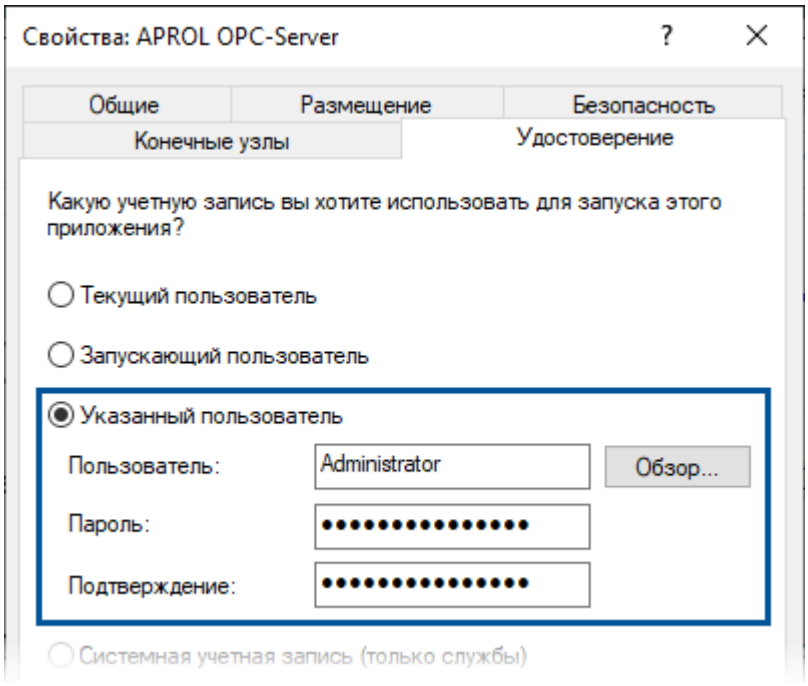
19.4. Настройка связи сервера APROL OPC-Server с модулем OPC DA Client

Чтобы настроить связь сервера APROL OPC-Server с модулем OPC DA Client:

1. В окне Службы компонентов выберите узел `Корень консоли → Службы компонентов → Компьютеры → Мой компьютер → Настройка DCOM → APROL OPC-Server`.
2. В контекстном меню узла `APROL OPC-Server` и выберите пункт **Свойства**.

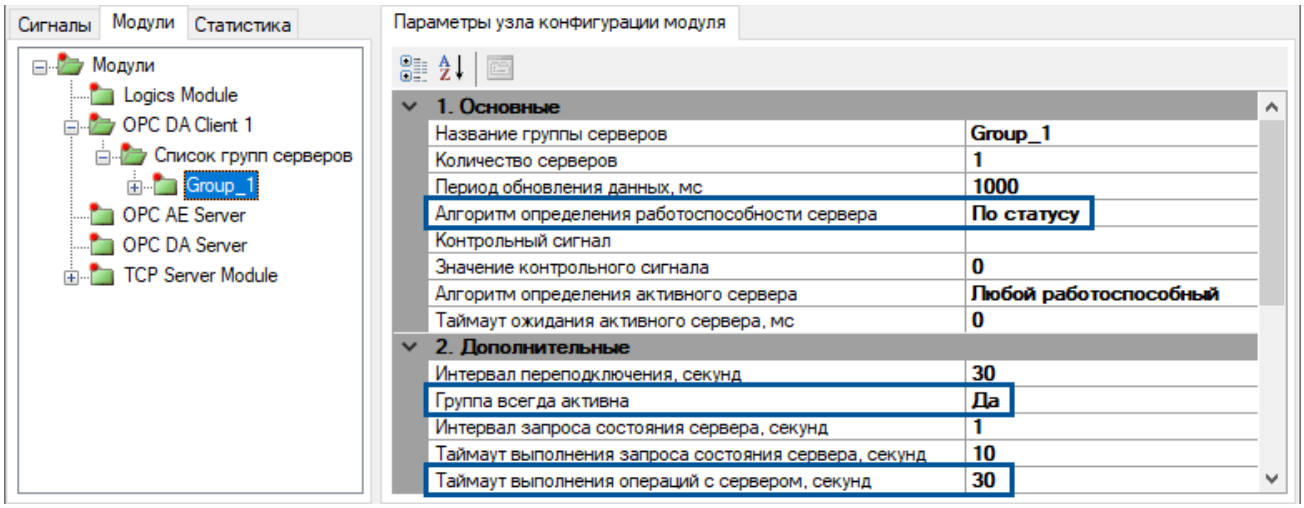


3. В открывшемся окне **Свойства: APROL OPC-Server** на вкладке **Удостоверение** установите переключатель **«Указанный пользователь»** и укажите данные учётной записи, из-под которой будет запускаться APROL OPC-Server.



4. В конфигурации SePlatform.Data Server для модуля OPC DA Client настройте параметры группы:

- параметру **Алгоритм определения работоспособности сервера** установите значение **«По статусу»**;
- параметру **Группа всегда активна** установите значение **«Да»**;
- параметру **Таймаут выполнения операций с сервером, секунд** установите значение **«30»** или более.



20. Работа в ОС Linux

Некоторые продукты Систэм Платформ могут работать на компьютерах под управлением ОС семейства Linux (в документации на продукты - ОС Linux). Такие продукты поставляются в виде `*.deb` и `*.rpm` пакетов и после установки функционируют в виде сервисов.

Ниже приведена общая информация для всех компонентов, работающих в ОС семейства Linux.

ПРИМЕЧАНИЕ

Подробности о том, работает ли компонент в ОС семейства Linux и название его пакета/сервиса смотрите в документации на конкретный компонент.

Поддерживаемые ОС семейства Linux

- Ubuntu
- Astra Linux
- РЕД ОС
- ALT Linux

Установка/удаление

В РЕД ОС (rpm-пакеты):

- Установить пакет:

```
sudo rpm -i <имя пакета>
```

- Удалить пакет:

```
sudo rpm -e <имя пакета>
```

В ALT Linux (rpm-пакеты):

- Установить пакет:

```
sudo apt-get install <имя пакета>
```

- Удалить пакет:

```
sudo apt-get remove <имя пакета>
```

В Ubuntu, Astra Linux (deb-пакеты):

- Установить пакет:

```
sudo dpkg -i <имя пакета>
```

- Удалить пакет:

```
sudo dpkg -r <имя пакета>
```

Пути

Директория расположения сервисов:

- РЕД ОС, ALT Linux:

`/usr/lib/systemd/system`

- Ubuntu, Astra Linux:

`/lib/systemd/system`

Директория установки:

- Для всех ОС семейства Linux:

`/opt/SePlatform/<имя продукта>`

(Astra Linux) Список сервисов

1. Откройте **Панель управления**.
2. Выберите группу **Система**.
3. Перейдите в раздел **Инициализация системы**.

Команды работы с сервисами

- Запустить сервис:

```
sudo systemctl start <имя сервиса>
```

- Остановить сервис:

```
sudo systemctl stop <имя сервиса>
```

- Перезапустить сервис:

```
sudo systemctl restart <имя сервиса>
```

- Текущее состояние сервиса:

```
sudo systemctl status <имя сервиса>
```

- Посмотреть журнал:

```
sudo journalctl -u <имя сервиса> -n <количество> -f
```

где:

- -n <количество> - вывести последние n строк строк журнала (опциональный атрибут).
- -f - выводить журнал в режиме реального времени (опциональный атрибут).

(Astra Linux) Подключение установочных репозиториев

Монтирование образа диска

Если диск с ОС смонтирован в CD-ROM, дополнительных действий не требуется.

Если ОС была установлена с помощью загрузочного Flash-носителя:

1. Скопируйте образ диска в виде `*.iso` файла на жёсткий диск в отдельную директорию (директорию монтирования).
2. Подключите образ диска:

```
sudo mount -o loop <путь до образа>.iso /<директория монтирования>
```

Подключение внешних репозиториев

1. Перейдите в директорию `/etc/apt` и откройте файл `sources.list`.
2. Добавьте строку:

```
deb [trusted=true] file://<путь до директории монтирования> <директории с
дистрибутивами>
```

где <директории с дистрибутивами> - список директорий, перечисленных через пробел.

3. Обновите базу данных пакетов:

```
sudo apt update
```

ПРИМЕЧАНИЕ

Подробнее о подключении репозиториев с пакетами в ОС Astra Linux:
https://wiki.astralinux.ru/pages/viewpage.action?pageId=3276859

20.1. (Astra Linux) Создание пользователя Operator с ограниченными правами

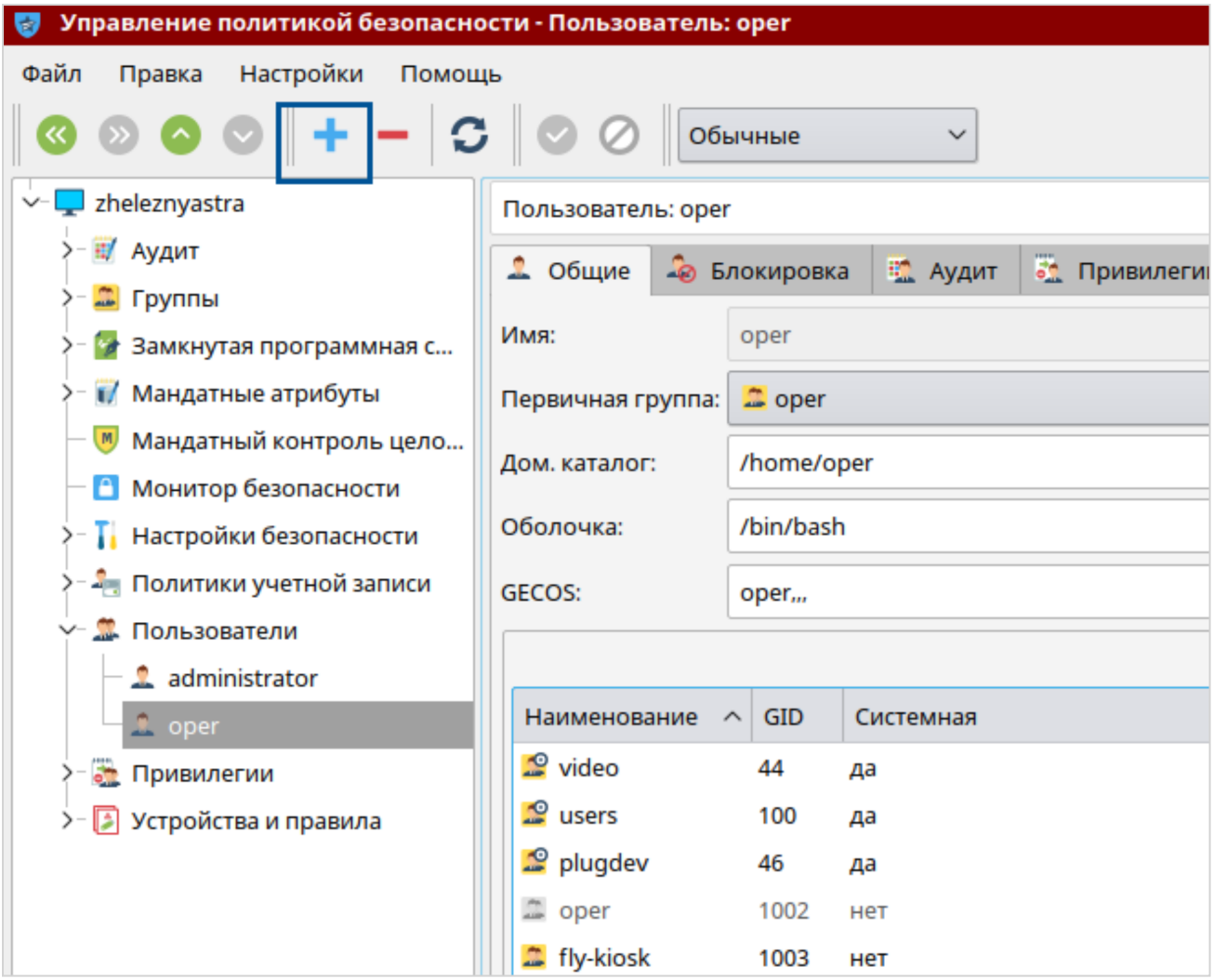
Откройте панель управления (меню `Пуск`).

Создание пользователя

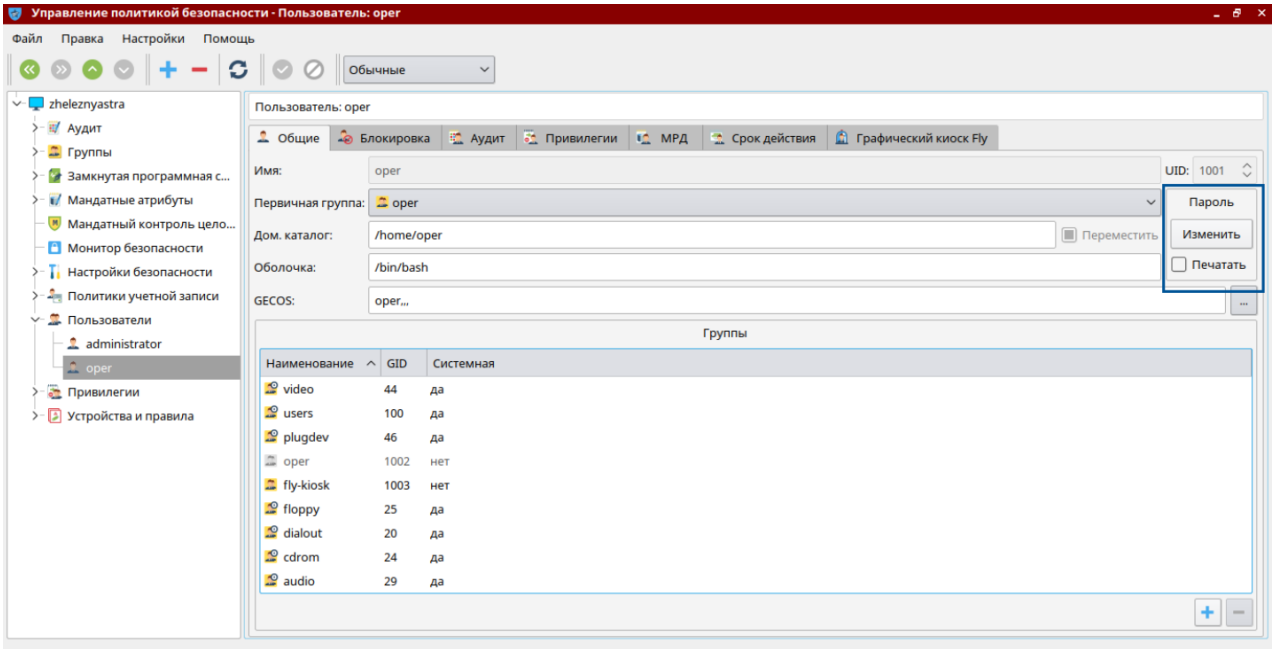
1. Перейдите в группу **Безопасность**.
2. Откройте раздел **Политика безопасности**.
3. Перейдите на узел **Пользователи**.

4. Добавьте нового пользователя кнопкой .

Укажите имя пользователя и подтвердите добавление.



5. Задайте первоначальный пароль пользователя, нажав кнопку **Изменить**.



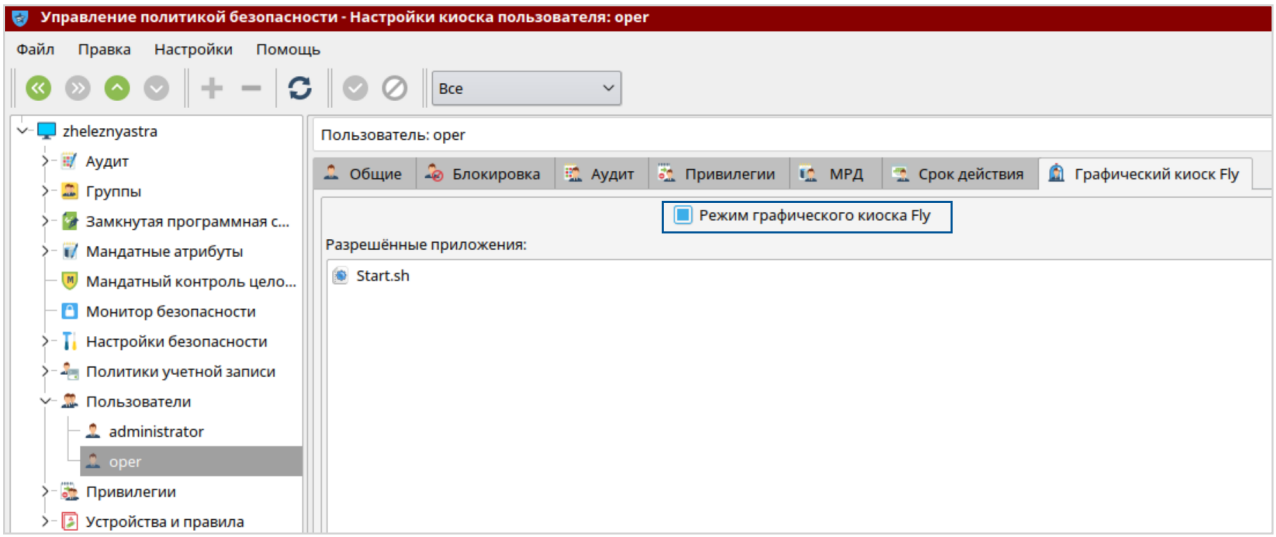
6. Установите права пользователя (подробнее **«F1»**).

ОБРАТИТЕ ВНИМАНИЕ

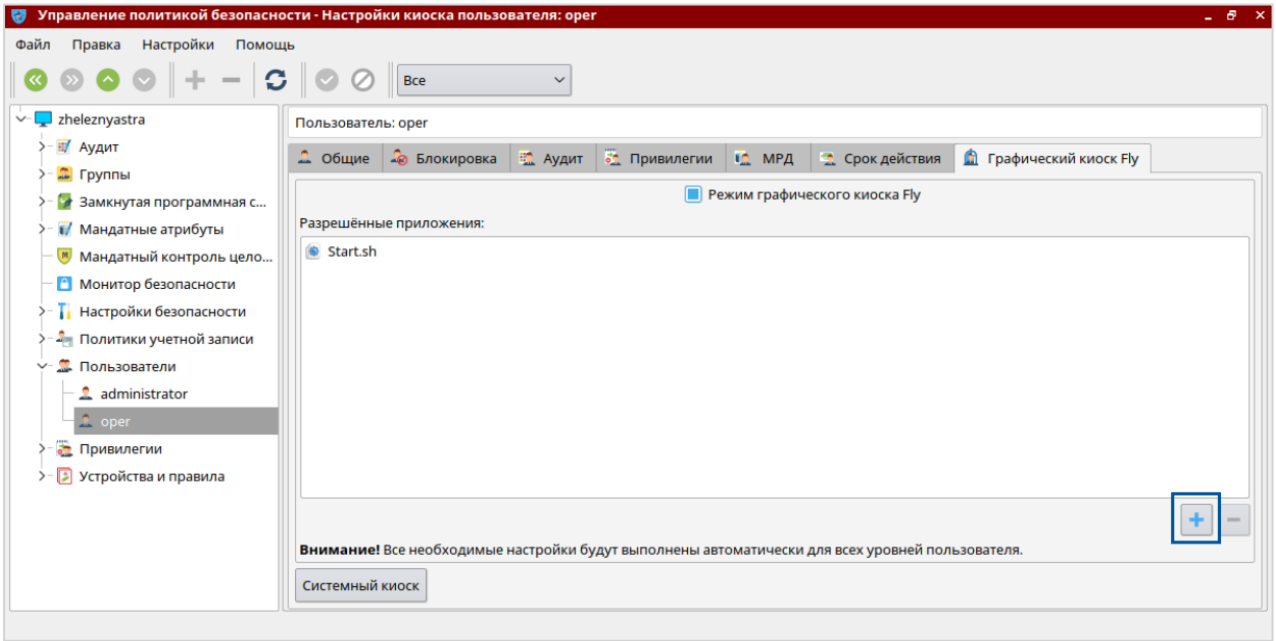
Для создания домашнего каталога нового пользователя необходимо хотя бы один раз войти в систему под этим пользователем.

Настройка режима графического киоска

1. Создайте скрипт для запуска приложения (например, проекта SePlatform.HMI).
2. Перейдите в группу **Безопасность**.
3. Откройте раздел **Политика безопасности**.
4. Перейдите на узел **Пользователи**.
5. Перейдите на вкладку **Графический киоск**.
6. Включите режим графического киоска.



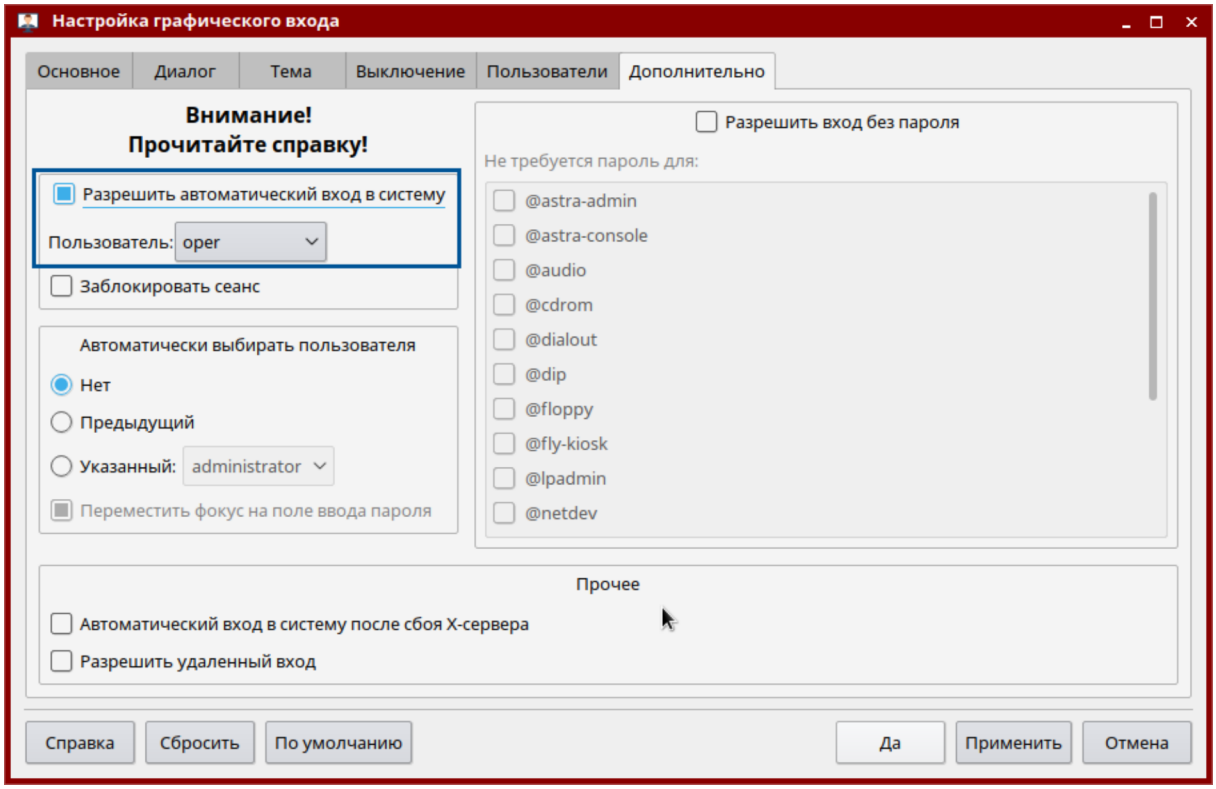
7. Добавьте разрешённое для выполнения приложение, нажав + и выбрав созданный скрипт.



8. Нажмите **Применить изменения** на панели инструментов.

Настройка автоматического входа пользователя

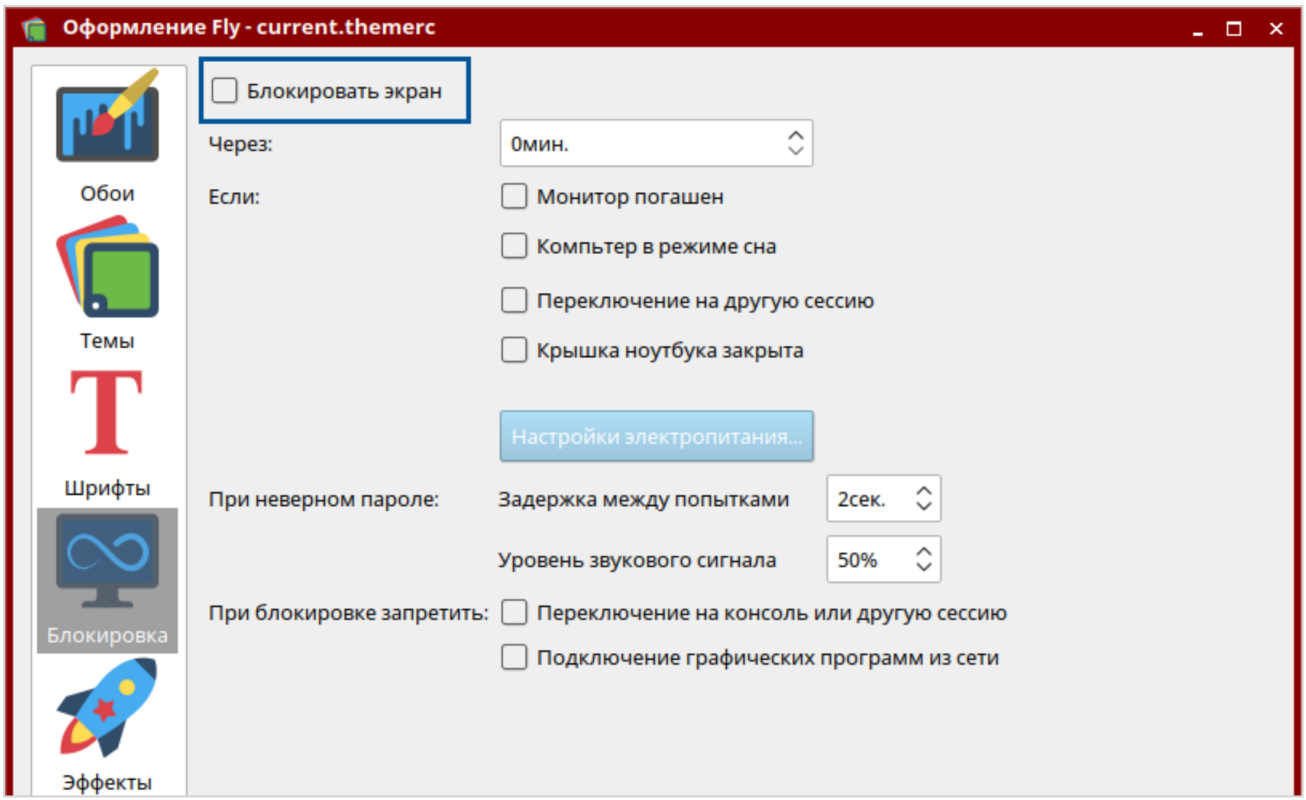
1. Перейдите в группу **Система**.
2. Откройте раздел **Вход в систему**.
3. Перейдите на вкладку **Дополнительно** и разрешите пользователю с ограниченным набором прав автоматический вход в систему.



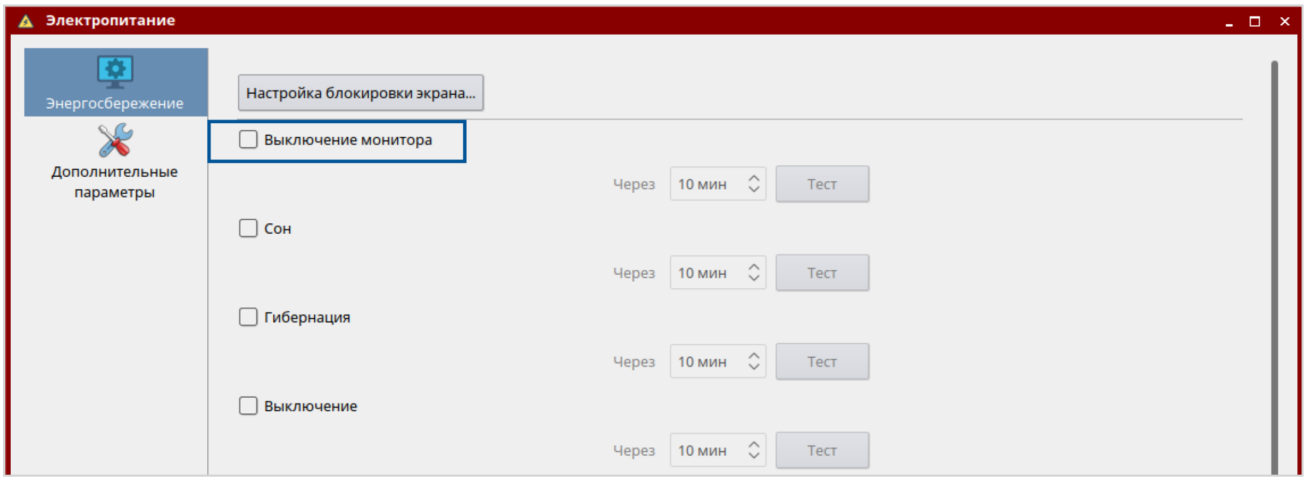
Настройка электропитания для выключения перехода в спящий режим при бездействии

1. Перейдите в группу **Система**.
2. Откройте раздел **Оформление Fly**.

3. Перейдите в группу **Блокировка** и снимите флаг **Блокировать экран**.



4. Нажмите кнопку **Настройка электропитания**.
5. В открывшемся окне снимите флаг **Выключение монитора**.



Запрет переключения между виртуальными терминалами

1. Перейдите в директорию настроек графической среды `/usr/share/X11/xorg.conf.d/`.
2. Создайте файл конфигурации с именем `50-novtswitch.conf`.
3. Запишите в файл следующие строки:

```
Section "ServerFlags"
Option "DontVTSwitch" "true"
EndSection
```

4. Перезагрузите операционную систему.

Разрешение переключения между виртуальными терминалами

1. Перейдите в директорию настроек графической среды `/usr/share/X11/xorg.conf.d/`.
2. Удалите созданный файл (стр. 157) конфигурации с флагом запрета.

```
sudo rm 50-novtswitch.conf
```

3. Перезагрузите операционную систему.

```
sudo shutdown -r now
```

История изменений

Редакция 2

- В главе Изменение учётной записи, от имени которой запускается служба изменены имена сервисов в ОС Linux для SePlatform.Data Server, SePlatform.AccessPoint и SePlatform.Historian (стр. 108).

Редакция 3

- Актуализированы описания подсистемы безопасности SePlatform.Security (стр. 33), приложения SePlatform.HMI.SecurityConfigurator (стр. 28) и модуля SePlatform.HMI.Security (стр. 31).
- Актуализированы рисунки в разделах 5. SePlatform.AccessPoint (стр. 15), SePlatform.Trends, SePlatform.Alarms и 8. SePlatform.HMI (стр. 21).

Редакция 4

- Добавлен раздел 19. Настройка DCOM (стр. 128).

Редакция 5

- В разделе Безопасное администрирование (стр. 106) обновлён перечень антивирусного ПО, совместимого с Систэм Платформ .
- Обновлен раздел Изменение учётной записи, от имени которой запускается служба (стр. 108) (в части ОС Linux):
  - Актуализировано описание смены пользователя для сервисов SePlatform.Data Server и SePlatform.AccessPoint.
  - Описание смены пользователя для SePlatform.Historian вынесено в отдельный блок.
  - Добавлен блок с описанием смены пользователя для сервиса агента SePlatform.License Server.
  - Обновлен порядок смены пользователя для SePlatform.HMI, SePlatform.HMI.Alarms и SePlatform.HMI.Trends.
  - Добавлена ссылка на документацию SePlatform.Security.

Редакция 6

- В разделе Изменение учётной записи, от имени которой запускается служба (стр. 108) (в части ОС Linux):
  - В инструкции смены пользователя для сервисов SePlatform.Data Server, SePlatform.AccessPoint и SePlatform.Domain в п. 13 добавлена команда export |grep DISPLAY.
  - Исправлены опечатки.

Редакция 7

- Актуализированы рисунки, исправлены опечатки.

Редакция 8

- Обновлены схемы в главах 2. Архитектура Систэм Платформ (стр. 7), 4. SePlatform.Historian (стр. 13), 5. SePlatform.AccessPoint (стр. 15).
- Актуализированы рисунки, исправлены опечатки.

Редакция 9

- Обновлен пункт Запрет переключения между виртуальными терминалами (стр. 157)
- В пункт Аппаратный ключ Guardant Sign добавлена инструкция по самостоятельной установке драйвера (стр. 39)

Редакция 10

- В раздел 16. Лицензирование Систэм Платформ добавлена информация по установке SePlatform.License Server в ОС Windows.
- В главе 18. Правила брандмауэра:
  - изменен порт получения исторических данных для компонентов SePlatform.HMI.Designer, SePlatform.HMI.Viewer, SePlatform.HMI.Alarms и SePlatform.HMI.Trends;
  - для компонентов SePlatform.Development Studio и SePlatform.Domain изменены порты для SePlatform.Net.Agent.

Редакция 11

- Внутренние изменения, исправлены опечатки.

Редакция 12

- Внутренние изменения, содржимое документа не изменилось.

Редакция 13

- Обновлена архитектурная схема SePlatform.Data Server (стр. 12).
- Актуализирована глава Работа в ОС Linux (стр. 151).
- Обновлен раздел Изменение учётной записи, от имени которой запускается служба (стр. 108).
- Для ключей Guardant указан адрес сервера обновления лицензий.